Joint Pub 6-02

Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems

1 October 1996

PREFACE

1. Scope

This publication provides command, control, communications, and computer (C4) systems doctrinal guidance across the range of military operations for those who:

a. Plan C4 systems support for joint operations;

b. Employ C4 systems in support of joint operations;

c. Provide operational and technical direction to C4 systems; and

d. Plan, manage, and employ C4 systems normally unique to Service or non-US forces as part of joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine (or JTTP) will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:

DENNIS C. BLAIR
Vice Admiral, US Navy
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

Table of Contents

APPENDIX

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the Impact of Joint Force Commander's Decisions on Command, Control, Communications and Computer (C4) Systems**
- **Provides Joint C4 Principles, Planning, and Management Considerations**
- **Considers Joint Task Force C4 Employment and Modular C4 Packaging**
- **Discusses Major Related C4 Systems and Support**

Introduction

Command, control, communication and computer (C4) systems support the joint force commander (JFC) and subordinate commands by providing the continuous automated flow and processing of information.

As driven by the mission, the foundations of the command, control, communications, and computer (C4) systems are laid by the command and control (C2) organization of forces assigned to the joint force commander (JFC). Specific command relationships and the organization of units, staffs, and battlespace drive the interconnecting communications methods and means. C4 systems must support this C2 organization in a complementary fashion and C4 systems must provide for the uninterrupted flow of information to and from commanders at all levels. **Based on the C2 structure**, C4 planners will **determine the systems that provide the most effective vertical and lateral information exchange** connectivity. These determinations provide the basic structure for the information exchange of the joint force. C4 planners will choose from the available resources those combinations which can be tailored to meet the mission support requirements. Typically, the combined system will provide voice, data, facsimile and video communications seamlessly and securely in an operator-friendly network. **The joint force C4 systems will allow force commanders to "pull" information from existing theater and national-level information services.** The warfighter's information "pull" coupled with the "smart push" of information by higher levels will provide the joint force commanders with an accurate and complete picture of their battlespace.

Joint Force Planning Factors and Structure Implications for C4 Planning

C4 planners must understand the JFC mission, intent, and concept of operations.

The C4 needs and capabilities of a small joint force with a limited humanitarian mission are vastly different from those of a combatant commander with continuing missions. Additionally, the different phases of a joint operation necessitate different and distinct levels of C4 assets and employment. C4 **planners also must have a comprehensive knowledge of the joint force structure and relationships.** The type of command relationships will dictate different information exchange needs. **C4 planning must be an integral part of the joint force command planning**. Reliable C4 is not planned in a vacuum; it has to be accomplished within the framework of established planning processes. **C4 planners must understand, expect, anticipate, and be prepared to deal with change**. The size, composition, and deployment of the joint force will vary as the level or form of operations escalate or decline in scope and intensity. C4 planners should **clearly understand the capabilities and limitations** of all potentially available **strategic, operational, and tactical C4 systems** and equipment, whether they are organic to Services and agencies, belong to non-US forces, are commercial, or are provided by a host nation.

Joint C4 Principles, Planning, and Management

The primary task of C4 systems is to ensure the continuous and automated flow and processing of information.

The joint warfighter's **C4 system must be flexible, interoperable, responsive, mobile, disciplined, survivable, and sustainable**. These principles provide the foundation on which the C4 planners build their systems and are applied during deliberate or crisis action planning. The joint force **C4 system provides the JFC the ability to control the flow and processing of information. It supports the JFC's decision making and provides the JFC with the capability to influence the action** during joint operations. The **mission, the JFC's intent, and the resulting concept of operations drive the joint force organization**.

The JFC requires the capability to obtain information from any location, at any time, and for any mission. The JFC and other warfighters must not be overwhelmed with voluminous amounts of information. They must have the capability to request and pull the information desired.

Planning Factors for the JFC and C4 Planners

The most important factors to consider in assessing a C4 plan are the adequacy of the C4 plan to satisfy the warfighters information requirements and whether or not the plan is feasible.

Reviewing the plan for **consistency with the C4 principles** as stated in Joint Pub 6-0, "Doctrine for Command, Control, Communications and Computers (C4) Systems Support to Joint Operations," is a useful first step. The JFC should determine if the C4 plans rest solidly on these principles and its ability to support the unit and mission. **Other factors to consider in evaluating a C4 plan are:** incremental building, modular C4 packaging, C4 interoperability, standardization, accommodating change, use of commercial capabilities, spectrum management, addressal of the level of training of operators of C4 systems, information protection, discipline, and timeliness.

Planning must proceed at various levels. The JFC's C4 planners perform **high-level planning to develop comprehensive C4 estimates**. The JFC's C4 **detailed planning** focuses on designing and engineering at the systems level; for example, radio transmission and message switching. The activation of C4 links and networks occurs when an operation order is executed. During the execution phase of an operation, **C4 planners must consider the next phase of the JFC's operational concept and plan for its support**. Certain operational considerations impose limitations on the use of selected C4 systems, including connectivity, range, and environment.

C4 Management

Joint C4 management indicates the exercise of systems and technical control over assigned communications systems.

C4 management allows the planners **to maintain an accurate and detailed status of the C4 network** down to the modular level. C4 management combines centralized control with decentralized execution and provides effective and efficient C4 support for the JFC's informational requirements. **Management organizations include Command, Control, Communications, and Computer Systems Division (J-6) as well as the Joint Communications Control Center (JCCC) and Services and Component Management.** The J-6 assists the commander in carrying out supervisory responsibilities for communications, electronics, and automated information systems. **The J-6 is responsible to the JFC for fulfilling the staff functions on all C4 matters. The J-6 establishes a JCCC to manage all communications systems deployed during joint operations and exercises.** Components and subordinate joint commanders establish C4 control centers to serve as their single point of contact and responsibility for joint C4 matters, and components and assigned support organizations should designate a single office

within their communications staffs to coordinate with the joint force staff J-6. Component C4 organizations should formulate and publish plans, orders, and internal operating instructions for the use of their component C4 systems.

Joint Task Force C4 Employment and Modular C4 Packaging

Joint task force (JTF) C4 planning and operational considerations depend upon the phases of a JTF military operation.

C4 planning and other related mission support activities take place in unison with the activation and subsequent phases of joint task force (JTF) operations. During the **predeployment phase,** the JFC is designated and forces are assigned. The Chairman of the Joint Chiefs of Staff warning and alert orders provide the JFC with guidance to initiate planning. The JFC issues a mission statement and commander's intent. Subsequent to the mission statement and commander's intent, the concept of operations is developed. During the **deployment phase,** the plan is completed and published. C4 assets incrementally deploy in support of the buildup in the operational area. Initial tactical communications is global, but minimal in capacity. Its primary focus is on decision support to the on-scene commander. In the **employment phase,** the JTF and the components continue to incrementally deploy. As these assets arrive they are added to the existing C4 system. The system increases in robustness and capability. During the **sustainment phase,** improvements are made to the C4 system. Changes in operation plans are accommodated using the in-place C4 system as the departure point. Repair parts and consumables, to include those necessary for preventive and routine maintenance, become an increasing concern. As in the predeployment phase, planning is the most important part of the **redeployment**. The C4 system must continue to provide information flow to the commanders, even as it purposefully disengages and large pieces of the system are removed and returned.

C4 Systems and Support

The JFC has the requirement to exchange information with the establishing authority, components, the Defense Information System Agency, home station, Department of State representative in the host nation, internal joint forces, and multinational forces.

After identifying the necessary support requirements, the C4 planner will select the system that supports the JFC's operational needs. **The following are some of the C4 systems that are available to the JFC and C4 planners to support joint force information requirements:** the Defense Information Infrastructure; Defense Information Systems Network; Federal Telecommunications System; Secure Voice System; Defense Commercial Telecommunications Network; Automatic Digital Network; Defense Message System; Defense Data Network; Defense Satellite Communications System; Military Strategic and Tactical Relay System; commercial satellite communications; military satellite architecture; Department of Defense Intelligence Information System; Defense Special Security Communications System; Joint Worldwide Intelligence Communications System; Joint Deployable Intelligence Support System; Frequency Resource Record System; Global Positioning System; Defense Satellite Program; Defense Meteorological Satellite Program; International Telecommunications Satellites; International Maritime Satellite System; Fleet Satellite Communications System; Public Switched Telephone Network; submarine cable; and the C4 systems of the Services.

CONCLUSION

This publication discusses the impact of the joint force commander's decisions on the employment of C4 assets to support joint and multinational operations. It covers the fundamental structural elements of C4 systems. It discusses the guidelines, basic tenets, and process for C4 planners to use in planning for the support for joint operations. It covers JTF C4 planning and operational considerations as they relate to the phases of a JTF military operation. Finally, this publication describes major related C4 systems and organizations.

Intentionally Blank

CHAPTER I
INTRODUCTION

"Joint doctrine offers a common perspective from which to plan and operate, and fundamentally shapes the way we think about and train for war."

Joint Pub 1, Joint Warfare of the Armed Forces of the United States

1. Purpose

This chapter provides the joint force commander (JFC) with the principal planning factors which govern the construction of a successful command, control, communications, and computer (C4) system to support the JFC's command and control (C2) information requirements. It speaks to the relationship that exists among the mission, the commander's intent, the selected C2 organization and the resulting C4 system. It provides information on the meaningful capabilities that any C4 system should provide the commander.

2. General

C4 systems support the JFC and subordinate commanders. These systems provide for the continuous automated flow and processing of information. This flow of information generates a common situational awareness, speeds decision making, and integrates the action of warfighters during mission execution.

3. Joint Force C4

a. **Joint Force Organization.** Joint forces are established on a geographic or functional basis at three levels: unified commands, subordinate unified commands, and joint task forces (JTFs). See Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)," for a detailed discussion.

- All joint forces include Service component commands and may also include functional component commands with operational responsibilities.
- The JFC has full authority to assign missions, redirect efforts, and direct coordination among subordinate commanders.

b. **Command and Control Structure.** As **driven by the mission**, the **foundations of the C4 system are laid by the C2 organization of forces** assigned to the JFC. Specific command relationships and the organization of units, staffs, and battlespace drive the interconnecting communications methods and means. C4 systems must support this C2 organization in a complementary fashion and, as indicated in Figure I-1, C4 systems must provide for the uninterrupted flow of information to and from commanders at all levels.

c. **Systems Requirements. Based on the C2 structure**, C4 planners will **determine the systems that provide the most effective vertical and lateral information exchange** connectivity. These determinations provide the basic structure for the information exchange of the joint force. C4 planners will choose from the available resources those combinations which can be tailored to meet the mission support requirements. Typically, the combined system will provide voice, data, facsimile, and video communications seamlessly and securely in an operator-friendly network. The major components will be mobile or transportable and can be assembled and very quickly put into operation. The C4 system can move as required and maintain connectivity among its users during such movement. The system may be modularized.

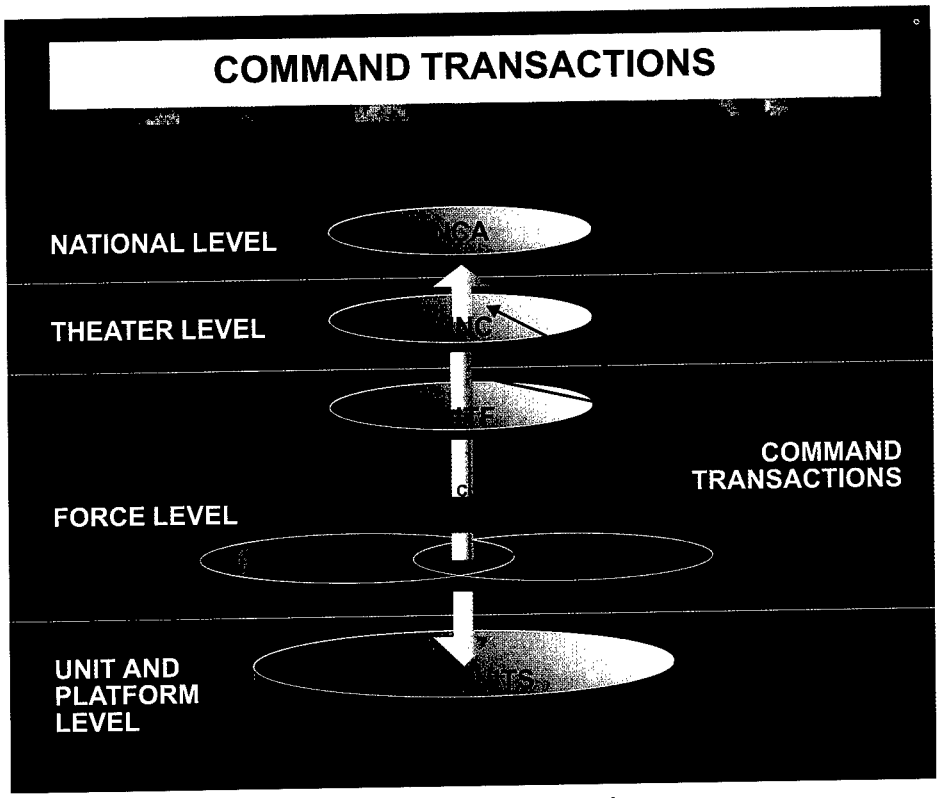


Figure I-1. Command Transactions

d. **Information, Resource and Targeting Transactions.** As depicted in Figure I-2, the **joint force C4 systems will allow JFCs to "pull" information** from existing theater- and national-level information services. The warfighter's information "pull," coupled with the "smart push" of information by higher levels, will provide the JFCs with an accurate and complete picture of their battlespace. As shown in Figure I-3, **these C4 systems will also provide sensor data directly to the warfighter**. This sensor information will provide commanders a common picture of the battlespace. Armed with the mission, the higher commander's intent, and this common picture, subordinate commanders can quickly and accurately engage the enemy.

e. **Changes. It is crucial that commanders and staff planners are sensitive to internal and external changes in their C2 organization.** Changes in levels of authority, the type of command relationships or other authorities, e.g., direct liaison authorized, all effect the overlaying C4 system.

> *"If I always appear prepared, it is because before entering on an undertaking, I have meditated and have foreseen what may occur. It is not genius which reveals to me suddenly and secretly what I should do in circumstances unexpected by others; it is thought and meditation."*
>
> **Napoleon I**

4. Joint Force Planning Factors and Structure Implications for C4 Planning

C4 planners must understand the JFC's mission, intent, and concept of operations. For example, the C4 needs and capabilities of a small joint force with a limited humanitarian mission are vastly different

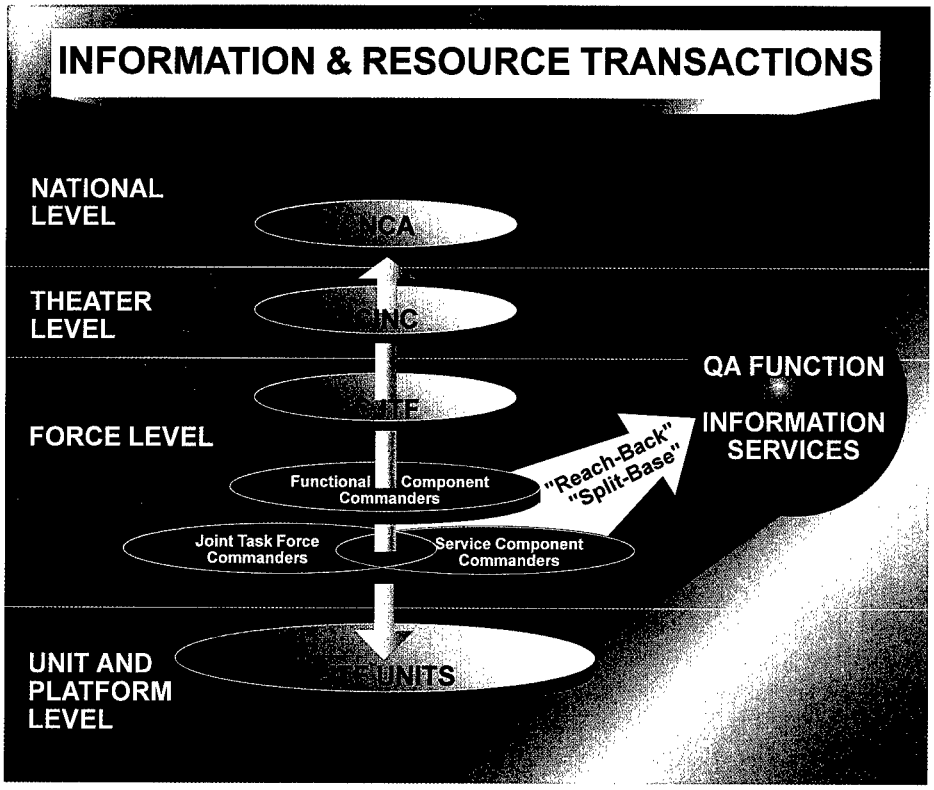


Figure I-2. Information and Resource Transactions

from those of a combatant commander with continuing missions. Additionally, the different phases of a joint operation necessitate different and distinct levels of C4 assets and employment.

a. **C4 planners also must have a comprehensive knowledge of the joint force structure and relationships.** The type of command relationships will dictate different information exchange needs.

b. **C4 planning must be an integral part of JFC planning**. Reliable C4 is not planned in a vacuum; it has to be accomplished within the framework of established planning processes.

c. **C4 planners must understand, expect, anticipate, and be prepared to deal with change**. The size, composition, and deployment of the joint force will vary as the level or form of operations escalate or decline in scope and intensity. The nature and the rate of fluctuation in the operational situation add to the C4 planner's challenges. The command's information requirements will change as the mission and the operational and tactical situations evolve.

d. C4 planners should **clearly understand the capabilities and limitations** of all potentially available **strategic, operational, and tactical C4 systems** and equipment, whether they are organic to Services and agencies, belong to non-US forces, are commercial, or are provided by a host nation. C4 planners should be aware of the following.

- **C4 doctrine, tactics, techniques, and procedures.** The **principles and practical mechanics** of how to best protect and move information **must be known and understood.**

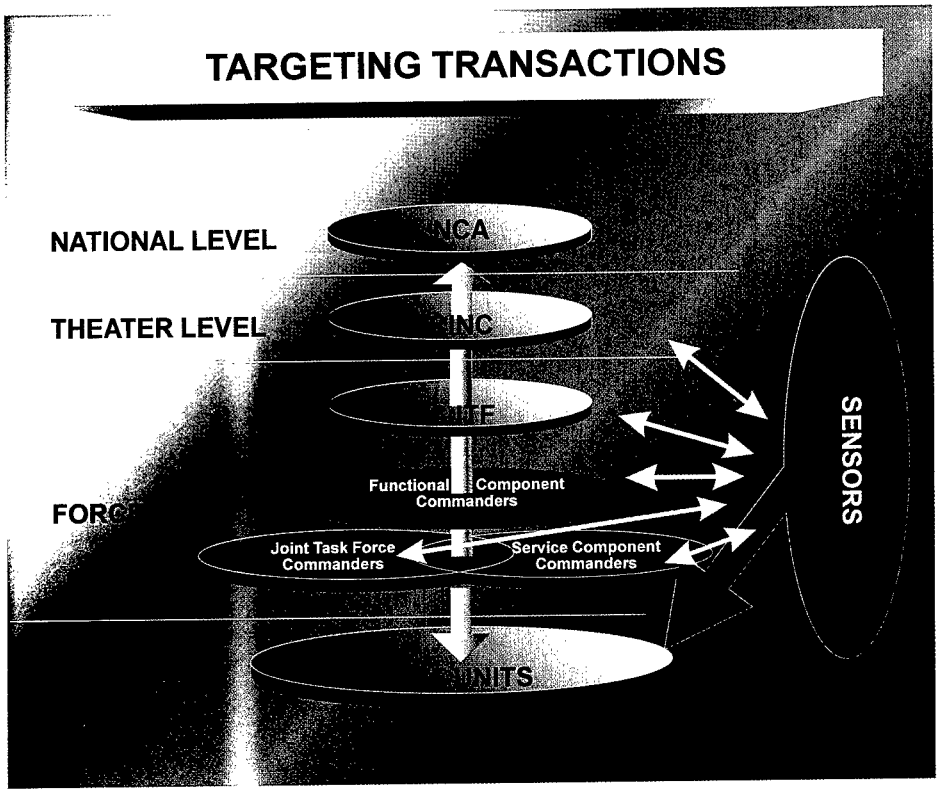


Figure I-3. Targeting Transactions

- Procedures for accessing and using systems to provide **global C4 connectivity**.

- Details of the **capabilities and limitations of assets controlled by the Chairman of the Joint Chiefs of Staff** (CJCS), including the Joint Communications Support Element (JCSE) and the process for obtaining its specialized communications support.

- **C4 capabilities and employment procedures of non-US forces**. As part of a multinational force, the US may have to provide the bulk of the C4, particularly to those multinational units above the tactical level. Release of hardware, software (operating systems and applications), data and communication networks, and C4 systems may be necessary when operating with multinational forces. **Release should not be accomplished unilaterally by in-theater personnel.** Such releases often require approval by the Secretary of Defense or coordination with the Secretary of State (see references DOD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," and CJCSI 6510.01, "Defensive Information Warfare Implementation").

e. **Multinational Organizations. Multinational organizations present special challenges.** C4 planners must ensure that communications links are established with non-US and host-nation commanders. **C4 interoperability is essential and can be accomplished through several means, including equipment interoperability, standardization, training, and liaison officers. The requirement for translators**

or other translation capabilities may become significant.

f. **Department of State Diplomatic Post.** Combatant commands must consider the early establishment of direct communications between the JFC and a United States diplomatic post using the most effective methods available. Communications capabilities and procedures for individual diplomatic posts are found in the diplomatic post's respective emergency action plan. Emergency action plan communications include (where available) high frequency (HF), International Maritime Satellite System (INMARSAT), tactical satellite (TACSAT), and ultra high frequency (UHF) or very high frequency (VHF) radios. The combatant commander should direct JTF communications based on the applicable emergency action plan after coordination with and approval by the Department of State.

Intentionally Blank

CHAPTER II
JOINT C4 PRINCIPLES, PLANNING, AND MANAGEMENT

"War acknowledges principles, and even rules, but these are not so much fetters, or bars, which compel its movement aright, as guides which warn us when it is going wrong."

Rear Admiral Alfred Thayer Mahan

1. Purpose

This chapter will provide the JFC with detailed guidelines with which to judge a C4 plan. It also provides C4 planners with specific planning factors to consider in planning and managing a successful C4 system. It also discusses the C4 management organizations of the JTF.

2. General

As discussed in Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," the primary task of a C4 system is to ensure the continuous, automated flow and processing of information. The joint warfighter's **C4 system must be flexible, interoperable, responsive, mobile, disciplined, survivable, and sustainable**. These principles provide the foundation on which the C4 planners build their systems and are applied during deliberate or crisis action planning. The joint force **C4 system provides the JFC with the ability to control the flow and processing of information. It supports the JFC's decision making and provides the JFC with the capability to influence the action** during joint operations.

a. The **mission, the JFC's intent, and the resulting concept of operations drive the joint force organization**. C4 plans which are based on C4 principles support this intent and concept of operations. Matching C4 capabilities to C4 requirements requires detailed planning. The resulting networks, nodes, and gateways also require responsive systems and technical control.

b. The C4 infrastructure must be able to do the following.

- **Support the flow and processing of information** across the range of military operations.
- **Support a smooth transition** from peace to any level of conflict.
- **Provide decision support** for maneuver, targeting, fire support, intelligence, air operations, logistics, and information warfare.
- **Support changes in the mission**, operational area, or the size, composition, command and control structure, or disposition of the forces. Combatant and component headquarters should always consider the likelihood that a single-Service operation will become joint or multinational. C4 planning must accommodate this possibility.

3. Commander's Joint Force C4 Requirements

The JFC and subordinate commanders require the capability to obtain information from any location, at any time, and for any mission. The JFC and other warfighters must not be overwhelmed with voluminous amounts of information. They must have the capability to request and pull

the information desired. Certain information must be disseminated widely in a push manner, such as warning of nuclear, biological, or chemical attack. Information must be resident with the JFC and the associated components or automatically updated as required. Information flow is not one way. The JFC and subordinate components also provide information both horizontally and vertically. The joint force's horizontal and vertical exchange of information must occur rapidly, providing support to the warriors upon demand.

4. Planning Factors for the JFC and C4 Planners

The most important factors to consider in assessing **a C4 plan** are the adequacy of the C4 plan to satisfy the warfighter's information requirements and whether or not the plan is feasible. Reviewing the plan for **consistency with the C4 principles** as stated in Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," is a useful first step. Other factors to consider in evaluating a C4 plan are as follows.

a. **Incremental Building.** Because military operations seldom occur at the same location as the preponderance of our military forces, **the JFC should expect to see C4 planners build the C4 system incrementally**. Most operations will initially rely on satellite communications to move information between headquarters and commanders. As the mission and assets allow, the C4 planners will install data and voice switching systems. Connections to the Defense Information Systems Network and commercial networks will become more extensive and robust. The system should also redeploy in an incremental fashion.

b. **Modular C4 Packaging.** Based on the mission, the commander's intent, the operation plan, the capabilities, limitations, and availability of equipment, and the C4 infrastructure in the operational area, the **C4 planner will build modular packages to meet the commander's needs**. C4 planners tailor these packages to existing conditions and link the individual C4 modules into a cohesive C4 system.

c. **C4 Interoperability. Interoperability should be achieved primarily by a commonality of equipment, software, and systems.** The C4 planner must know the capabilities and limitations of the other component C4 systems and must be able to integrate them into the joint C4 plan.

d. **Standardization. Standardization should be evident in the planned C4 system.** The planner should ensure that equipment strings and system configurations are standardized throughout employed units. The JFC's C4 requirements must not be compromised by uncontrolled, widespread use of nonstandard systems, protocols, procedures, or terminology. C4 systems

INTEGRATED TACTICAL AND STRATEGIC SWITCHING

Commercial, high-volume transmission systems...significantly enhanced throughput and enabled components to extend switched and dedicated voice and message trunks to many locations. Extensions of strategic circuits...allowed the component commands to turn their tactical satellite terminals back to direct support of combat operations.

SOURCE: Jean M. Slupik, "Integrated Tactical and Strategic Switching," in Alan D. Campen, editor, The First Information War

planners and operators must have a shared frame of reference.

e. **Accommodating Change.** C4 planners must anticipate change and be able to respond in a timely manner to variations in the initial mission. **The C4 plan should include a diversity of C4 systems. Connectivity among commanders, headquarters, and units must incorporate alternate routes and methods.** Ensuring this diversity of systems and alternate routes will contribute to the C4 systems' flexibility, survivability, and responsiveness.

f. **Commercial Capabilities.** The C4 plan should consider the use of commercial systems. The availability of **commercial C4 systems may offer an alternative means to satisfy the JFC's C4 needs and may reduce the number and size of deployed modular C4 packages**. Commercial capabilities that are resident in the operational area may allow C4 planners to compensate for tactical C4 system shortages and meet the early information requirements of a joint force deployment. The use of commercial C4 systems and networks may affect the planned mix of deployable C4 modules. C4 planners must ensure that the deployed modular packages include sufficient capabilities to interface with commercial systems.

"It cannot be too often repeated that in modern war...the chief factor in achieving triumph is what has been done in the way of thorough preparation and training before the beginning of war."

Theodore Roosevelt
Graduation Address, US Naval Academy, June 1902

g. **Spectrum Management. Frequencies allocated to critical functions must be identified and protected.** As frequencies may be claimed by various national or regional entities, significant potential exists for problems. To prevent such problems, the use of radio and radar frequencies at all organizational levels must be coordinated through national and international channels. Frequencies must be managed to reduce the likelihood for friendly electromagnetic interference (EMI). This is particularly important when multiple systems share the same frequency bands. The increasing use of frequency hopping radios further complicates the management process by spreading the potential for EMI throughout the operational area. The JFC Frequency Manager has essential responsibilities in spectrum management throughout the operational area and must be an integral part of the planning process.

h. **Training. The level of training of operators of C4 systems and managers should be addressed.** Resident training should complement the Joint Mission Essential Task List. The application of joint doctrine and tactics, techniques, and procedures defines the C4 requirements for training, exercises, equipment, and organization. C4 training should reflect the insights gained from past experience.

i. **Information Protection and C4 System Defense.** A critical aspect of effective C4 is the successful execution of information warfare (IW). IW applies across the range of military operations and at every level of warfare. Defensive IW (IW-D) integrates and coordinates protection and defense of information, information-based processes (including human decision making processes), and information systems (including C4 systems, weapon systems, and infrastructure systems).

- **IW-D Process.** The IW-D process integrates and coordinates policies and procedures, operations, and technology to protect information and information-based processes, and to defend information systems (including C4

systems). The objectives of IW-D are to ensure access to timely, accurate, and relevant information when and where needed, and to deny an adversary the opportunity to exploit friendly information and systems for their own purposes. Effective IW-D implementation ensures the availability, integrity, authentication, confidentiality, and non-repudiation of information. Effective IW-D ensures required service levels of information systems (and, through coordination, services provided by non-US Government entities). Figure II-1 illustrates the elements of the target set of information and information systems protected and defended by IW-D processes. Refer to the CJCS Instruction 3210.01, "Joint Information Warfare Policy," and to the CJCS Instruction 6510.01, "Defensive Information Warfare Implementation."

- **Elements of the IW-D Process.** IW-D occurs within the context of four inter-related processes: information environment protection process, attack detection process, capability restoration process, and attack response process. Figure II-2 illustrates the IW-D implementation process.

- **Information Environment Protection Process.** Information and information system protection is critical to the military's ability to conduct operations and is the responsibility of information producers, processors, and users. Information protection applies to any medium and form including hardcopy

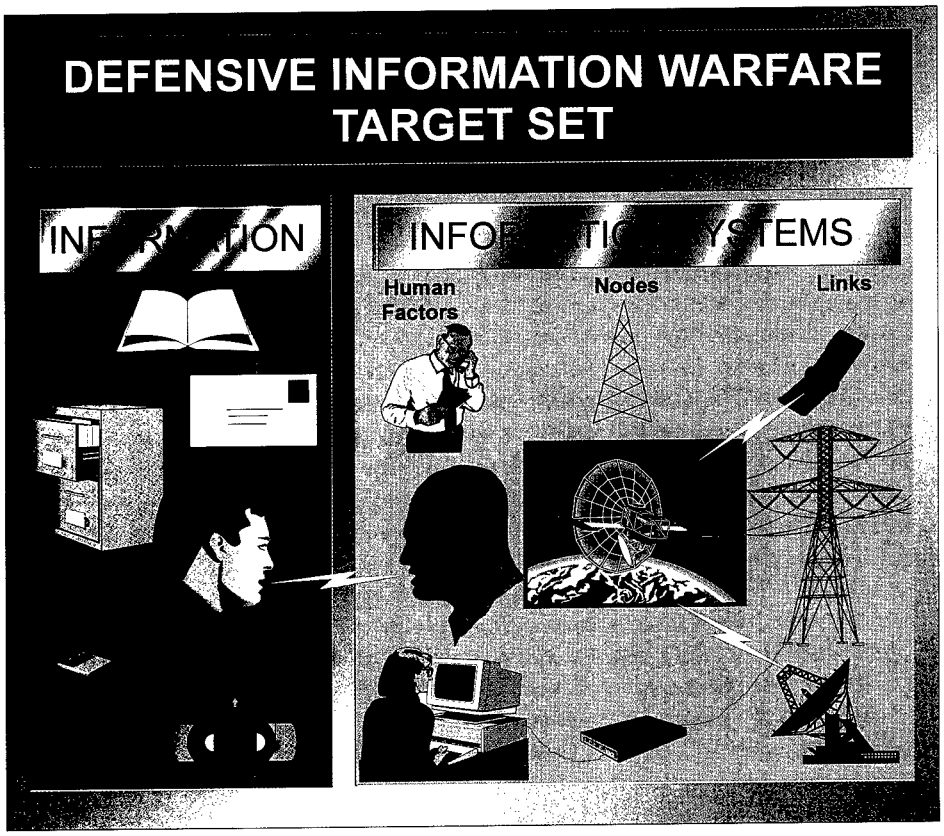


Figure II-1. Defensive Information Warfare Target Set

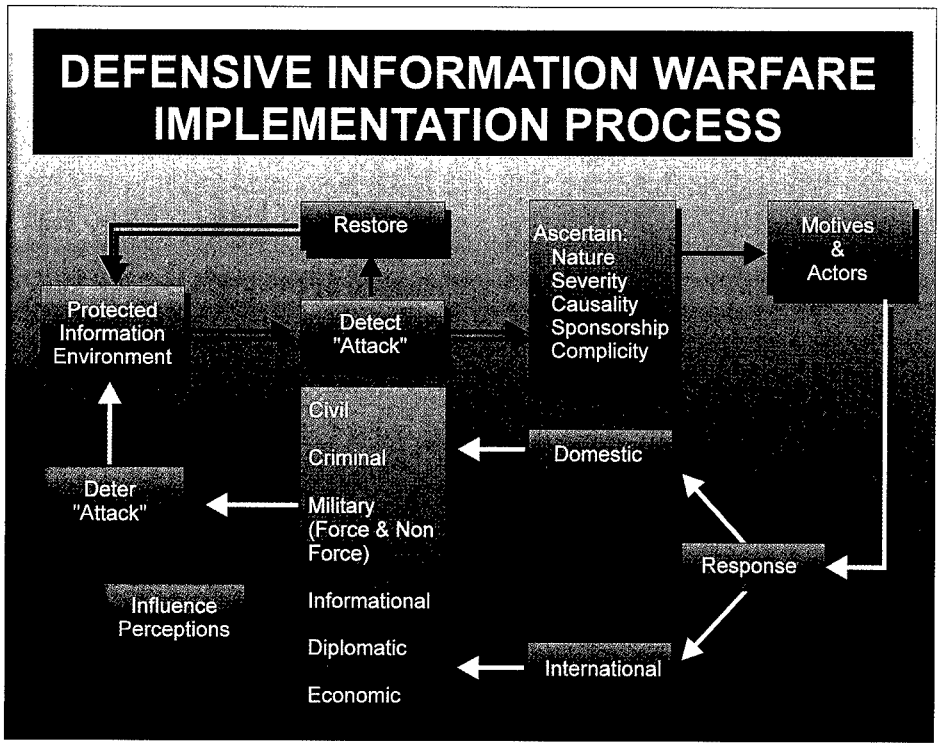


Figure II-2. Defensive Information Warfare Implementation Process

(message, letter fax), electronic, magnetic, video, imagery, voice (telephone, including cellular), telegraph, computer, and human. Information protection ensures the availability, integrity, authenticity, confidentiality, and non-repudiation of information.

- **Attack Detection Process.** The attack detection process requires close cooperation and/or coordination among information system developers, vendors, administrators, users, service providers, law enforcement, and intelligence agencies. The speeds at which information system attacks occur have outpaced our ability to detect and respond via human means. An automated way to assess the severity (including system damage, information compromise, and malicious logic insertion) and to mitigate these effects is essential to effective IW-D. Timely attack detection and reporting is key to initiating the restoration and response processes.

- **Capability Restoration Process.** The capability restoration process relies on pre-established mechanisms for prioritized restoration to minimum essential capabilities. Capability restoration may rely on backup and/or redundant links or system components, backup data bases, or even alternative means of information transfer.

  •• In some cases, required technical restoration capabilities are beyond the abilities of the affected sites. On-line or deployable restoration assistance capabilities provide required expertise and tools to restore services. Common types of restoration assistance are the computer emergency response team and security incident response capability.

These restoration assistance programs exist at the Defense Information Systems Agency (DISA), the Services, and commercially.

•• Automated alerting mechanisms provide system managers and administrators with enhanced situational awareness and create decision points. Immediate termination of adversary system access to protect against further actions and information exploitation must be weighed against the needs of the legal and intelligence communities to collect against and exploit the adversary for effective implementation of the response process. A decision to allow the adversary to maintain access in order to gather information for the response process relies on a risk assessment of continued access and consideration of current and future operational and intelligence impact.

•• A key step in the restoration process is to inventory system resources to identify adversary leave-behind capabilities.

•• Finally, post-attack analysis provides information about vulnerabilities exploited and leads to security improvements. Automated recording or capturing of specific attack techniques during the incident can provide information required for analysis.

- **Attack Response Process.** The attack response process involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action(s) against perpetrators. The process contributes to information environment protection by removing threats and enhancing deterrence.

j. **Discipline.** C4 systems and resources are limited. The JFC should ensure that the information moving over these limited **resources supports necessary decision making and overall mission execution.** The mission and the commander's intent will, to some extent, guide what information is provided to the joint force. The commander should provide additional guidance on what information is to be "pushed" and "pulled" to the JTF from the "global grid." Consideration should be given to using long-established procedures such as "MINIMIZE."

k. **Timelines.** The C4 **systems goal should be the transfer of information in real time**; that is, as the event happens. The JFC can assist in making this goal a reality by identifying all critical information requirements. These requirements should be listed by priority levels, allowing timely restoration of the most critical information in case of outages.

Information Warfare
CJCSI 3210

Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.

Figure II-3. Information Warfare

"Unless a staff officer is able to assist his commander in getting things done, in addition to coordinating, planning and policy making, he is not serving his full usefulness."

General Alexander M. Patch
Quoted in Ray S. Cline,
Washington Command Post, 1951

5. C4 Planning

In Chapter I, "Introduction," the important planning factors for the joint force and their general implications for the C4 planners were outlined. The following section further refines C4 planning processes.

a. **Additional C4 Planning Characteristics and Tasks**

- **The planning process must commence as soon as possible.** It is essential that all staff planners get involved in the planning process early. The process is continuous and iterative. Planners employ the C4 principles to guide their activities, structure tasks, and determine solutions to C4 requirements.

- Planning must proceed at various levels. The JFC's C4 planners perform **high-level planning to develop comprehensive C4 estimates**. The JFC's C4 **detailed planning** focuses on designing and engineering at the systems level (for example, radio transmission and message switching). The activation of C4 links and networks occurs when an operation order is executed. During the execution phase of an operation, **C4 planners must consider the next**

- Certain operational considerations impose limitations on the use of selected C4 systems. These considerations include the following.

  •• **Connectivity.** The comprehensive **linking of C4 systems establishes a level of connectivity** which enables communication to and from the joint force and its users. To the maximum extent possible, the hardware and software **interfaces should be transparent to the system user**. The continued flow of information should not depend on action by an intermediate user.

  •• **Range. Range will continue to be a factor in connecting the nodal points and networks.** Equipment capabilities and the distance between nodal points must be considered.

  •• **Environment. The C4 system must be tailored for the environment** to include hydrographic, terrain, meteorological, vegetation, manmade structures, and cultural features. Such environmental surroundings determine the usable frequencies, output power, and location of C4 systems.

b. **C4 Planning Methodology.** The C4 **planning process** is divided into five areas: mission analysis, information needs analysis, interoperability and compatibility analysis, capabilities analysis, and allocation of C4 assets.

- **Mission Analysis. "What is the desired military end state?"** The **key** to answering this question is found in the **commander's intent, concept of operations, and C2 organization**. C4 planners must clearly understand the C2 structure and how the operation will

phase of the operation. A thorough and coordinated mission analysis must be performed by C4 planners. The specified and implied tasks, coupled with the concept of operations and commander's intent, will provide the framework for a C4 structure. **The C4 structure identifies elements that need to exchange information and, subsequently, C4 systems terminations.** Having a plan that readily allows for expansion is vital.

- **Information Needs Analysis.** Information needs analysis answers the question, **"Who needs to exchange information with whom?"** The information exchange requirements identify the products to be transmitted and received and the throughput, quantity, and characteristics of those products. This occurs for each phase of the operation.

- **Interoperability and Compatibility Analysis. This analysis identifies technical protocols, formats, data fields, operational, and security considerations.** Global C4 support depends upon the national systems as well as tactical, commercial, and host-nation telecommunications systems. These systems must exchange information. Personal intervention and procedural fixes have been the methods of choice to resolve interoperability and compatibility issues. Such measures are not adequate for the long term, and must give way to equipment-level solutions. Equipment, connectivity, and procedural standards must allow for the "seamless" transmission of information to the user. Mission success rests, to a great extent, on interoperability.

- **Capabilities Analysis.** Based on the mission analysis, information needs, and interoperability and/or compatibility analysis, **the planner identifies the C4 systems required to support the operation plan.** C4 planners match information requirements with capabilities and assets. The capabilities analysis **matches the means** of communication **with the operational needs.** The result of this analysis identifies specific C4 systems requirements. Some suggested guidelines follow.

  •• **Strongly consider the use of the commercial infrastructure** when feasible. Commercial systems can add capability and optimize the use of military resources. In addition to technical issues, planners and operators must consider contractual arrangements and the associated costs.

  •• In lieu of or in conjunction with commercial systems, employ military terrestrial systems as a second alternative. This reserves military C4 systems for the strategic and tactical requirements to which they were originally designed.

  •• Use strategic and tactical satellite communications only when terrestrial systems cannot meet user requirements. Operate satellite systems as a last resort. This limited resource should be employed in those critical situations where no other means can fulfill the requirement.

- **Allocation of C4 Assets.** Having identified the C4 requirement, the C4 planner **must examine all available resources and plan a tailored C4 system.** To employ all available C4 resources, planners must be familiar with Department of Defense (DOD) and subordinate policies, directives, and publications. These documents give the planner specific information on C4 organizations who support the JFC. Some guidelines for allocating C4 assets are as follows.

  •• **Establish the basic C4 system prior to the arrival of joint forces.**

•• Employ additional equipment and reconfigure connectivities to **provide direct routing to principal organizations** in the operational area.

•• **Provide alternate routing.** Alternate paths increase the robustness of a network and prevent site isolation. Alternate routing must be provided to principal organizations and to the maximum extent possible, to other subordinate organizations of the joint force.

•• Have sufficient equipment and technical personnel on hand for **rapid response to new missions and critical outages**. Establish single points of contact at each termination site to troubleshoot network problems.

c. **Spectrum Management.** C4 planners **must manage the use of the electromagnetic spectrum**. They must ensure that frequency usage requirements are met and deconflicted and they must ensure that compatible frequencies are incorporated into communications-electronics annexes, communications-electronics operating instructions, and joint communications-electronics operating instructions (JCEOIs). When networks become active, C4 managers must monitor the frequency spectrum for electromagnetic interference. Planners and controllers must resolve conflicts and, as necessary, reallocate and reassign frequencies.

d. **Space-Based Asset Management.** Key in the commander's ability to gather information and to command and control an operation is his ability to exploit all of his assets. Assets that operate in space are critical to fully understand and exploit. These assets include communications, imagery, weather, geographic intelligence, and other related systems. In order to fully exploit these resources they must be managed properly and deliberately. Special individuals are available to incorporate these assets into the C4 plan.

e. **Planning Tools.** Generally, communications **requirements are categorized by the volume of information to be transmitted**, the speed of service desired, the destination(s), the transmission media, and the security classification of the information. **The most difficult factor to estimate is volume.** Volume comprises the quantity and length of transactions to be transmitted. The volume of traffic a circuit can handle depends upon its type and capacity. Capacity represents the size of the circuit.

- **Manual Planning Techniques.** A C4 systems planner can use manual methods to help refine the C4 support requirements. These include the following.

•• **Structural Analysis.** Structural analysis is the foundation of communications architecture studies. Given the time and information, this methodology is probably **the best way to define communications trunking and switching requirements** and long-term C4 needs. Depending on the degree of detail, the technique can yield estimates of varying precision. Structural analysis consists of the following steps. (1) Define the general environment, distances involved, geography, and commercial infrastructure. (2) Evaluate the enemy's capabilities. (3) Identify the information required to perform the mission and tasks, such as commander's intent, concept of operations, and organizations involved. (4) Develop information flow in terms of connectivity and information characteristics. Determine who must communicate with whom and the volume, type of traffic, security classification, and frequency of reporting. (5) Finally, translate functional and information flow requirements into performance requirements. How much and

how fast do particular users need the information?

•• **Stated Requirements.** This method relies on obtaining system performance and usage estimates from questionnaires and interviews. This technique is only **applicable** when an **operational baseline system exists** and **when interviewed personnel have experience** operating, maintaining or, in the case of warfighters, being supported by this system. The stated requirement technique is easier than collecting actual traffic measurements. The disadvantage of the stated requirements approach is that it may be skewed by subjective inputs or interpretations, while the traffic measurement approach relies upon specific, objective inputs.

•• **Traffic Flow Experience.** This technique involves **using historical usage data** as the basis for developing requirements estimates. The planner uses data to lay out the topology of the baseline system and establish the network traffic flow. This model is modified through the use of expert input as necessary to reflect the parameters of the projected system. (1) There are difficulties associated with measuring communications baseline usage during specific situations and then applying that data in hypothetical situations. The **assumption** implicit in this technique is that **historical data or current usage is indicative of actual communications needs.** (2) **Traffic records are available more often for fixed and commercial communications systems** than for tactical or mobile systems. These fixed systems, which are primarily common-user systems, usually have data available for the number of attempts over a specified accurately indicate user communications requirements. (3) **Historical usage is not necessarily a good indication of future requirements.** Only communications needs that are supported can be measured. Historical usage data ignores any unfulfilled needs and does not differentiate between "essential" and "nice-to-have" communications needs. **The adage that system use expands to fill capacity generally holds true.** (4) The **strength of this technique** is in its reliance on accurately measured **data** rather than on perceptions.

•• **Rule of Thumb.** This technique is used primarily by commercial system architects who **rely on past experience** for the design of systems serving customers who often share similar needs.

- In a broad sense, the allocation of telecommunications resources in a military environment can be correlated to "standard" needs. During the force structuring process for a operational area, it is a normal procedure **to allocate resources according to force size and composition.** C4 planners simply allocate the "normal" (rule of thumb) communications support to a command based on previous requirements and experience. **That allocation is usually a good starting point for a more detailed analysis.**

- The final communications requirements estimate will probably result from a combination of techniques, including structural analyses, statements of user requirements, computer-based simulations, and experienced intuitive judgment. **The combined use of the various approaches will help to develop precise estimates.** Basic warfighter requirements

- While forecasting essential traffic is an important factor in sizing military communications systems, there are other relevant factors. In particular, **alternate routing or added capacity** must be included. This added capacity will allow the C4 Systems Division (J-6) to maintain **critical communications despite possible system degradation**. The reliability of user services will vary depending on wartime conditions, the level of use, and atmospheric conditions. Planning, alternate routing, and additional system capacity will mitigate these fluctuations and provide the necessary support. **The planned capacity of the C4 system must meet the needs of a wartime system.**

f. **Development of Network Plan.** After the planners identify a system which satisfies the JFC's informational requirements, they coordinate with the transportation planners to ensure a successful deployment. Finally, **they begin detailed planning to interconnect modular C4 nodes and gateways into the systems and the network**. The network is now defined in terms of C4 nodes, gateways, and associated systems keyed to operational mission phases and deployment schedules.

g. **Continuous Planning. C4 planners must continuously update their plans**, even after implementation. C4 packages and the activation of the C4 system must continually be tailored to changing mission situations. Once the C4 networks have been activated, C4 staffs must manage the existing network and plan future actions.

6. C4 Management

Joint C4 management indicates the exercise of systems and technical control over assigned communications systems. C4 management allows the planners **to maintain an accurate and detailed status of the C4 network** down to the modular level. C4 management combines centralized control with decentralized execution and provides effective and efficient C4 support for the JFC's informational requirements.

a. **Management Organizations**

- **Command, Control, Communications, and Computer Systems Division.** The J-6 assists the commander in carrying out supervisory responsibilities for communications, electronics, and automated information systems. **The J-6 is responsible to the JFC for fulfilling the staff functions on all C4 matters.** This includes the development of C4 architectures and plans, as well as policy and guidance for the integration and installation of operational C4 systems. **The J-6 formulates policy and guidance for all communication assets supporting the JFC.** The J-6 and his or her staff assist the JFC in publishing C4 plans, annexes, and operating instructions. They review C4 plans prepared by subordinate component commanders, manage the frequency spectrum within the operational area, and coordinate with host-nation authorities.

- **Joint Communications Control Center (JCCC). The J-6 establishes a JCCC to manage all communications systems deployed during joint operations and exercises.** Components and subordinate joint force commanders establish C4 control centers to serve as their single point of contact and responsibility for joint C4 matters. **The JCCC, as an element of the J-6, exercises control over all deployed communications systems.** The JCCC serves as the single control agency for the management and operational direction of the joint communications network. As discussed in detail in the CJCSM 6231 series, the JCCC performs planning, execution, technical direction, and management

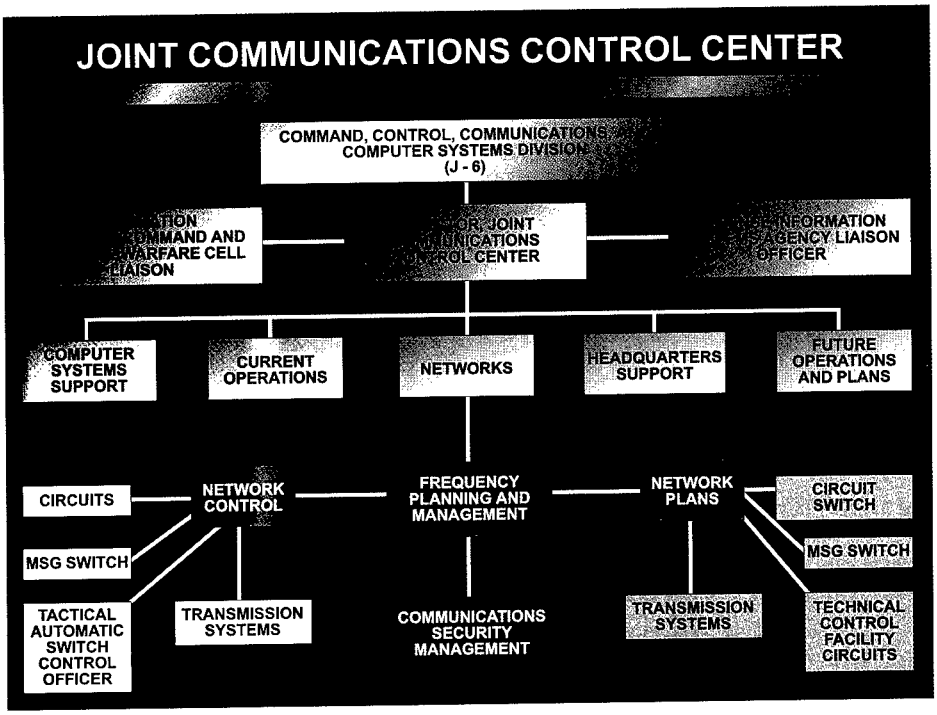


Figure II-4. Joint Communications Control Center

functions. Figure II-4 depicts a notional Joint Communications Control Center.

- **Services and Component Management.** Components and assigned support organizations should designate a single office within their communications staffs to coordinate with the joint force staff J-6. Component C4 organizations should formulate and publish plans, orders, and internal operating instructions for the use of their component C4 systems. The Services and components may have different designations **for their communications control facilities that manage their deployed C4 assets**. The Army, Air Force, Marine Corps, Navy and Joint Special Operations Task Force (JSOTF) normally refer to their component communications control centers as systems control (SYSCON). All of the component's technical control facilities perform network control and reconfiguration. For example, they change circuit channelization, direct trouble shooting to resolve problems, and provide status information.

b. **Management Implementation.** When C4 networks are activated, C4 planners and operators begin monitoring the status of the systems, networks, and nodes. They **implement corrective actions to restore any outages**. User-detected C4 system problems are reported to the user's immediate chain of command and supporting SYSCON. SYSCON directs the technical control facility. The technical control facility then resolves the problem or coordinates with other technical control facilities and the user's chain of command to solve the problem.

- Technical control **facilities continually monitor and evaluate the condition of the C4 system**, with attention to such aspects as inter-nodal connectivity, trunks, and circuits. Technical control facilities receive status information from

the system operators and local monitoring equipment. They regularly test trunks and circuits for compliance with technical and quality specifications.

- **The technical control facilities maintain a current status of key systems, circuits, communications-electronics facilities, and major modular C4 packages.** The **technical control facilities** also report this information to the JCCC and SYSCONs through technical management and direction channels.

- C4 planners at the **JCCC and the components use status information to obtain an operational profile of the C4 network and to identify problem areas and solutions**. Planners may reconfigure the network to maintain C4 connectivity and adequate user support. Status information can also assist in planning network expansions or contractions by identifying critical circuits and alternate routing.

c. **The Joint Spectrum Management System (JSMS). The JSMS is a personal computer-based application** which supports the JTF and component spectrum managers. This application includes a planning template, frequency assignment data base, equipment characteristics data base, and a collection of engineering tools to calculate the effects of current and proposed spectrum use on the electromagnetic environment.

Intentionally Blank

CHAPTER III
JOINT TASK FORCE C4 EMPLOYMENT AND MODULAR C4 PACKAGING

"The Services put more electronic communication connectivity into the Gulf in 90 days than we put in Europe in 40 years."

Lieutenant General James S. Cassidy
J-6, The Joint Staff

1. Purpose

This chapter discusses the various phases of a joint operation and the communications consideration during each phase.

2. General

a. The notional JTF used in the following paragraphs is made up of an Army Corps, a Numbered Air Force, a Marine Expeditionary Force, a Navy Battle Group, and a JSOTF.

b. **C4 planning takes place in unison with the phases of JTF operations.** Applicable operational phases include predeployment, deployment, employment, sustainment, and redeployment.

3. Predeployment

The JFC is designated and forces are assigned. The Chairman's warning and alert order provides the JFC with guidance to initiate planning. The JFC issues a mission statement and commander's intent. Subsequent to the mission statement and commander's intent, the concept of operations is developed.

a. **The C4 Objective.** Produce a plan to support the commander's intent, mission, and concept of operations.

b. **The C4 Method.** Using the planning methodology previously discussed in Chapter II, "Joint C4 Principles, Planning, and Management," the C4 planner will develop a "rough" plan that supports the commander. Automated aids, historical data, previous experiences, and intuitive judgment will assist in developing the initial plan. Subordinate organizations must be contacted early in the planning process. The planning is conducted concurrently with subordinate organizations. Joint force C4 planners supply subordinate organizations decisions and information as it becomes available. Close contact is maintained with supporting defense agencies such as the DISA, and supporting unified commanders such as the US Transportation Command.

c. **The C4 Means.** This phase of the operation will rely almost exclusively on the installed commercial and government communications infrastructure.

4. Deployment

The C4 system must continue to provide information flow to the JTF and component commanders, even as it purposefully deploys and large pieces of the system are moved towards the operational area. The plan is completed and published. **C4 assets incrementally deploy in support of the build-up in the operational area.** Initial tactical communications is global, but minimal in capacity. Its primary focus is on decision support to the on-scene commander.

a. **The C4 Objective.** Provide for the continuous flow of information between commanders during the initial phases of the operation.

b. **The C4 Method.** Lift assets will deploy the initial JTF C4 capability. This initial C4 capability is comprised of a modular package which provides the commander's voice and data connectivity. The system is global and provides a logical point from which to incrementally build the remainder of the system. The initial system is not robust and may be severely degraded when disturbed.

c. **The C4 Means.** This phase of the operation will rely on UHF satellite, commercial and/or military super high frequency (SHF) satellite, extremely high frequency (EHF) satellite, and other commercial assets to support strategic and long-haul communications requirements. VHF, HF, and UHF radios assets are used extensively by subordinate units for internal information requirements.

5. Employment

The JTF and the components continue to incrementally deploy. As these assets arrive, they are added to the existing C4 system. The system increases in robustness and capability.

a. **The C4 Objective.** Produce a C4 system which provides for the automated flow and processing of information.

b. **The C4 Method.** As dictated by the mission, commander's intent, the concept of operations and, to a certain extent, lift assets, more capable C4 systems arrive and are added to the initial network. Large capacity satellite, terrestrial switching, and transmission systems arrive. Numerous alternate routes are established which substantially increase the robustness of the network. Local area networks (LANs) abound and connection to JTF and global wide area networks (WANs) vastly increase information flow. The network increases in complexity, necessitating more sophisticated systems and technical control.

c. **The C4 Means.** This phase of the operation will rely on whether large capacity ground mobile forces (GMF) compatible and commercial satellite systems will connect to the global grid. SHF and UHF terrestrial multi-channel radio will connect voice and data via digital switches and technical control facilities. Maximum use is made of existing commercial and government systems.

6. Sustainment

Improvements are made to the C4 system. Changes in operation plans are accommodated using the in-place C4 system as the departure point. Repair parts and consumables, to include those necessary for preventive and routine maintenance, become an increasing concern.

a. **The C4 Objective.** Sustain and improve the automated flow and processing of information to the commanders.

b. **The C4 Method.** As guided by the continuing mission, the needs of the commander, and the users, changes are made to the constructed C4 systems. These changes improve the overall capacity of the system to seamlessly and transparently move information among components and national organizations. Less-than-perfect circuit design is corrected. As design faults are corrected and the C4 system becomes increasingly reliable, attention is turned to those actions which will keep the system functioning. Preventive and routine maintenance, stockage of spare and/or repair parts and consumables demand increasing attention.

c. **The C4 Means.** JCCC directs changes in the C4 system in response to changing mission requirements and user demands or complaints. Technical control facilities take on an increasingly important role as they make

changes in the established systems without interrupting service to the customers. Organic and common-user transportation assets move consumable and repair parts to established repair facilities.

7. Redeployment

As in the predeployment phase, planning is the most important part of the redeployment. The C4 system must continue to provide information flow to the commanders, even as it purposefully disengages and large pieces of the system are removed and returned.

a. **The C4 Objective.** Disassemble and return the unnecessary C4 systems while simultaneously providing automated information flow and processing to the JFC.

b. **The C4 Method.** The easiest way to visualize the redeployment phase is to play the previous three phases in reverse. Sustainment capability will decrease. Redundant systems will redeploy, followed by the high capacity satellite and terrestrial systems. In the final days of this phase, the C4 systems may look very similar to that which originally deployed. Planning is as critical for the smooth redeployment of a C4 system as it was for the initial deployment.

c. **The C4 Means.** The original commercial and government infrastructure should support as much of the C4 redeployment as possible. Lacking such an infrastructure, the last systems to redeploy will likely be the mobile, easily transportable assets, such as UHF single-channel and small SHF satellite terminals.

8. Summary

The five phases of JTF operations are highly situation- and mission-dependent. Timelines between phases may be severely compressed, with the actual deployment occurring prior to completion of all of the predeployment planning. Employment might follow so quickly on the heels of deployment as to appear simultaneous. Redeployment could easily be the predeployment phase of a follow-on operation. In other words, these phases do not follow each other in lock-step. They do, however, provide a benchmark, a guide post, for the JFC and J-6 planner.

Intentionally Blank

CHAPTER IV
C4 SYSTEMS AND SUPPORT

"No matter where we fight in the future, no matter what the circumstances, we will fight as a joint team. We will have fingers on the team that are individual Services, but when it comes to the fight we want the closed, clenched fist of American military power. The days of single Service warfare are gone forever."

Admiral David E. Jeremiah, USN
Vice Chairman of the Joint Chiefs of Staff, 12 June 1993

1. Purpose

This chapter describes major related C4 systems and organizations which may be employed in support of joint operations.

2. General

The JFC has the requirement to exchange information with the establishing authority, components, DISA, home station, US Department of State representatives in the host nation, internal joint forces, and multinational forces. After identifying the necessary support requirements, the C4 planner will select the system that supports the JFC's operational needs. The following are some of the C4 systems which are available to the JFC and his C4 planners.

3. Defense-Wide and Joint C4 Systems

a. **Defense Information Infrastructure. The defense information infrastructure encompasses the information transfer, processing, storage, manipulation, retrieval, and display resources of the Department of Defense.** The defense information infrastructure is the interconnected system of computers, communications equipment, data, applications, security, people, training, and other support structures which serve the local and worldwide information needs of the Department of Defense. The defense information infrastructure connects users through voice, data, video, and multimedia services.

b. **Defense Information Systems Network (DISN). The DISN is a subelement of the defense information infrastructure.** The DISN provides the end-to-end, consolidated worldwide telecommunications infrastructure for information transfer in support of military operations. Its operation is not overtly apparent to end users. It facilitates information resource management and is responsive to national security and defense needs under all conditions. The DISN will establish a seamless, secure, robust, agile, reliable, and cost-effective telecommunications network **that will satisfy** all of the DOD end-to-end information needs. This C4 system will allow the JFC to **globally focus his efforts at the point of conflict** and dominate the battlespace.

- The DISN provides long haul, end-to-end common-user and dedicated voice, data, and video service. It provides the connectivity for secure and nonsecure communications. **The DISN architecture prescribes a global network** which integrates existing DISA assets, military and commercial satellite communications, and leased telecommunications services as well as the existing worldwide telecommunications infrastructure.

c. **Federal Telecommunications System (FTS) 2000.** FTS 2000 is the telephone and data system of the US Government. It is interoperable with DISN and the Defense Commercial Telecommunications Network in the continental United States (CONUS), Hawaii, and the US territories. The General Services Administration participates in management of FTS 2000. FTS 2000 provides the following services to the Department of Defense.

- Switching and transmission service for common-user voice.
- Transmission of compressed and full-motion video.
- Switching and transmission service for raw or packeted data.
- Switching and transmission service for systems requiring high data rates or the use of the Integrated Services Data Network.

d. **Secure Voice System (SVS).** The SVS uses the transmission and switching capabilities of the DISN and the public packet switched network to provide an improved worldwide secure voice capability. SVS improves the DOD worldwide secure voice capabilities by using secure telephone unit III (STU III) terminals and expanding the number of subscribers, via bridges, to the Defense Red Switch Network. SVS also provides point-to-point secure voice, secure conference calling, and interface capabilities in support of the National Command Authorities (NCA) and the Department of Defense.

e. **Automatic Digital Network (AUTODIN).** AUTODIN is a store-and-forward message switching network controlled by DISA. It is designed to meet the operational requirements of the Department of Defense. AUTODIN consists of AUTODIN switching centers, Service and Defense agency processing facilities, and a variety of terminal facilities. Automated Message Processing Exchanges (AMPEs) provide limited switching functions for attached AUTODIN terminals. Additionally, AMPEs provide for the conversion of destination names into internal AUTODIN addresses and the criteria based distribution of messages. Local and unit telecommunications centers are the principal entry and exit points for AUTODIN messages.

f. **Defense Message System (DMS).** DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically. DMS combines messaging and electronic mail using x.400 protocol and addressing x.500 directory service to increase the speed and capacity of messaging. DMS adds reliability, security, and a worldwide directory capability supporting the interface of tactical message systems with commercial and allied message systems. DMS will be the only message system in the Department of Defense.

g. **Defense Data Transport.** The defense data transport is composed of three separate networks: Military Net - unclassified level, Internet Protocol Router Network (NIPRNET) - Sensitive but Unclassified, Internet Protocol Router Network (SIPRNET - Secret Level), Joint Worldwide Intelligence Communications System (JWICS - Top Secret Level). User communities are separated based on security levels and high speed commercial carriers. Each classified subnet is protected by encryption devices on each trunk. The means for achieving the multi-level network include special security devices at the user system connection points. Special security devices are also used at packet switched nodes and the automated key distribution centers. This approach converts older, physically separated networks into logically separate subnetworks.

h. **Global Command and Control System (GCCS)**

- GCCS is the key command, control, communications, computers and intelligence (C4I) system in satisfying the C4I for the Warrior concept. It provides a fused picture of the battlespace within a modern C4 system capable of meeting warfighter needs into the 21st century. GCCS incorporates the core planning and assessment tools required by combatant commanders and their subordinate JFCs and meets the readiness support requirements of the Services. In moving the joint C2 support capability into the modern era of a client-server open architecture, GCCS brings to the ongoing DOD C4I migration strategy the essential tools for the Services and agencies to successfully reduce the large number of systems in use today. GCCS is a user-focused program under the oversight of the Office of the Secretary of Defense and the Joint Staff.

- At each GCCS site, one application server is configured as the executive manager (EM) providing LAN desktop services. It also hosts applications not loaded on the data base server. The EM server acts as the user interface, providing access to GCCS applications through user identification and discrete passwords. GCCS software applications are categorized in four groups: Kernel, Common Operating Environment (COE), common, and mission applications.

i. **Military Satellite Communications Architecture.** As indicated by Figure IV-1 the military satellite communications architecture provides a wide range of capabilities to the JFC and the C4 planner. The architecture consists of both commercial and military satellite capabilities. No one sub-architecture can effectively satisfy the wide range of communications services required by the Department of Defense and agencies. Access to Military Satellite Communications (MILSATCOM) is governed by CJCS Memorandum of Policy 37, "Military Satellite Communications Systems."

- The UHF Satellite Communications System is comprised of the fleet satellites (FLTSATs), leased satellites (LEASATs), Gapfiller satellites, and UHF-Follow On (UFO) satellites. These satellites are positioned to provide UHF satellite communications from 70 degrees north and 70 degrees south latitudes over four service areas: CONUS, Atlantic Ocean, Indian Ocean, and the Pacific Ocean. The constellation requires two satellites in each service area. The system provides a variety of low capacity long haul, point-to-point, broadcast, and netted single-channel communication links among mobile and shore units. Each UFO satellite provides 39 discrete channels with frequencies ranging from 240 to 320 megahertz (MHz). Selected UFO flights will include an EHF package compatible with Military Strategic and Tactical Relay System (MILSTAR).

- Defense Satellite Communications System (DSCS). DSCS provides multi-channel communications services and is the only DOD-wholly-owned military long-haul communications system. It provides worldwide, responsive, wide band and, under special circumstances, portions of DSCS and can provide anti-jam service satellite communications supporting critical national, strategic, and tactical C4 requirements. DSCS is the backbone for high-capacity C2, intelligence, and multi-channel communications service among users worldwide, to include the NCA, the White House Communications Agency, Diplomatic Telecommunications Service,

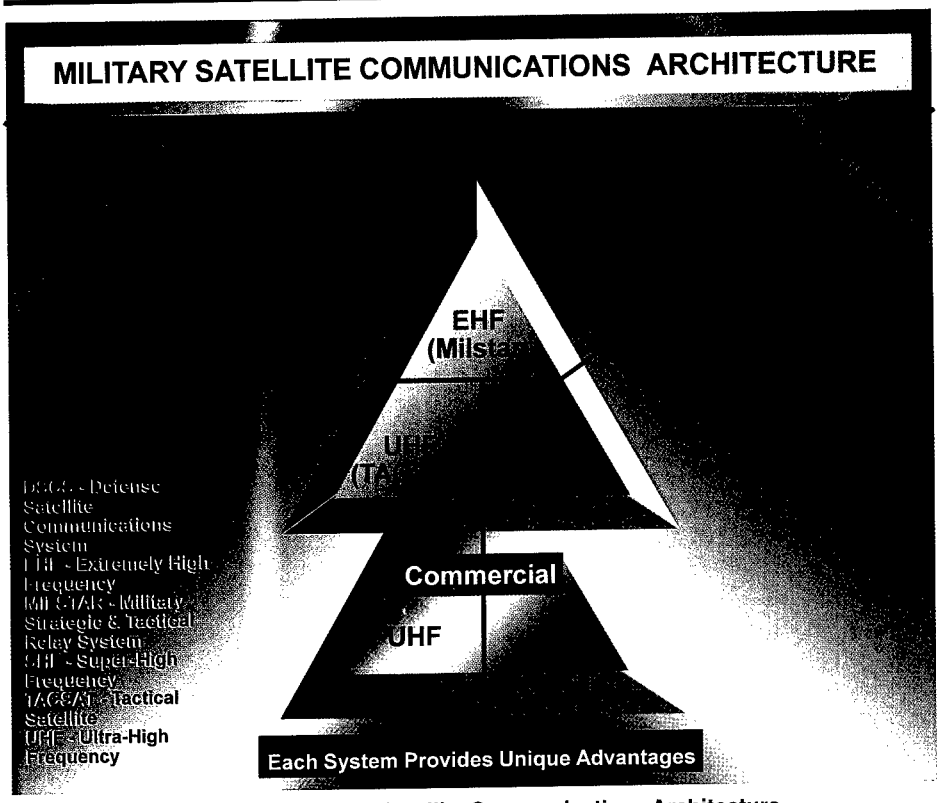


Figure IV-1. Military Satellite Communications Architecture

the Department of Defense, national government agencies, and our allies. The DSCS constellation consists of five primary DSCS-III satellites and six residual satellites, (DSCS-III and DSCS-II). DSCS III supports jam-resistant secure communications for emergency action message dissemination, missile warning, integrated tactical warning and attack assessment information, and NCA, Joint Chiefs of Staff, and combatant commander conference calling. The mission of the DSCS is to support the tactical, deployed warfighter. The Navy uses DSCS to provide high-capacity communications to capital ships. Joint force elements should consider satisfying long-haul strategic requirements with commercial systems before turning to the DSCS, as DSCS is oriented toward forward deployed operational forces.

- **Military Strategic and Tactical Relay System.** The MILSTAR satellite system provides a survivable and enduring warning to and control of strategic forces during and after nuclear attack. In addition, MILSTAR provides robust communications to tactical forces and is less susceptible to nuclear effects or jamming than DSCS. To ensure continued availability, MILSTAR satellites incorporate a variety of survivability features. MILSTAR provides significant protected medium data rate capability to deployed operational forces and extends MILSATCOM support to Army echelons below corps. Polar EHF coverage requirements are satisfied by payloads on polar host satellites.

- **Global Broadcast Service (GBS).** GBS provides a revolutionary advancement in

satellite communications. GBS fills two key needs of the warfighter. It provides high data rate service to many users at once and high delivery rates to very small, low cost user receive-only terminals. GBS reduces the need to send information more than once to reach multiple users and thus reduces the overall burden on existing communications means. No other current DOD satellite provides this capability. The interim GBS capability consists of four high-capacity transponders on selected UFO satellites.

- **Commercial Satellite Communications.** The joint force's growing communications requirements will increase reliance on the use of commercial satellite systems. The use of commercial satellite communications requires advance planning and coordination with DISA. DISA manages leasing arrangements, host-nation approval, and frequency allocation. Lease and operating costs must be considered and added to operational planning documents. The Commercial Satellite Commercial Initiative bulk leases commercial transponders for direct management by the Department of Defense through a Broadcast Management Center. This arrangement reduces costs and increases responsiveness to changing DOD needs. The primary commercial satellites used by the Department of Defense are International Telecommunications Satellite (INTELSAT) and INMARSAT.

•• **International Telecommunications Satellites.** INTELSAT is an international enterprise of over 120 member countries and is the largest commercial system in the world. Its network consists of 19 satellites on-orbit and is projecting a fleet of 33 by 1997. Commercial satellite (COMSAT) is the US signatory and owns just over 20% of the INTELSAT systems. There is nothing in the INTELSAT agreement that prevents the Department of Defense from using this system for military purposes, and the President has emergency powers over COMSAT's facilities and operations.

•• **International Maritime Satellite System.** With headquarters in London, England, the INMARSAT organization has 74 member nations. It operates a constellation of four satellites and leased transponders on other commercial satellites. Originally designed for maritime use, INMARSAT has grown to be a popular system for mobile applications. There are restrictions concerning the use of INMARSAT by combatant elements. Planning should consider these restrictions listed in the reference INMARSAT Convention, 16 Jul 79.

j. **Department of Defense Intelligence Information System (DODIIS). DODIIS is a worldwide computer network which links intelligence data handling systems.** These systems support the collection, production, and dissemination of various defense intelligence products. DODIIS consists of approximately 40 nodes and is characterized by various means of intelligence input processing, including imagery exploitation, electronic intelligence, communications intelligence, and human intelligence.

k. **Defense Special Security Communications System (DSSCS).** The DSSCS uses the same systems as the AUTODIN. Traffic separation is provided at the various AUTODIN

both part of DSSCS. The special intelligence communication network is a dedicated family of circuits, terminals, and facilities that serve the Special Security Office functions at most major headquarters worldwide.

l. **Joint Worldwide Intelligence Communications System.** JWICS is high speed (up to T-1/1.544 megabytes per second [Mbps]) communications system designed to provide secure, top secret and sensitive compartmented information (SCI) data, interactive video teleconferencing, and video broadcasting capabilities subscribers. Subscribers to the system includes the unified commands, subordinate component commands of the unified commands, designated joint task forces, the Services, Service intelligence centers, science and technology intelligence centers, DOD agencies (e.g., Defense Intelligence Agency [DIA], Defense Mapping Agency, National Security Agency), and selected non-DOD agencies (e.g., Department of State, Federal Emergency Management Agency, and the White House). Video-capable subscribers will be able to conduct interactive, point-to-point, and multi-point video teleconferences with any one or combination of subscriber(s). All sites will have the capability to receive high-speed data transmissions (including bulk data files) and imagery. Sites will have access to data bases and will be capable of electronic publishing, in conjunction with the Joint Deployable Intelligence Support System (JDISS). INTELINK, available via JWICS, is an automated intelligence dissemination and collaboration medium that uses Internet technology in a secure communications environment. INTELINK provides uniform methods for exchanging intelligence among providers, and between providers and users of intelligence. INTELINK servers are updated periodically with a variety of intelligence products including video, imagery, and current as well as long-term intelligence production. Deployable JWICS are also available to support contingency operations. The JWICS gives Indications and Warning centers, Joint Intelligence Centers, and watch centers, including appropriately equipped ships afloat, the ability to share and discuss time-critical information worldwide. The JWICS uses primarily commercial satellite communications in combination with terrestrial transmission media. It also interfaces with the Washington, D.C., area's Secure Video Teleconferencing System and can transmit in collateral and SCI modes. DIA is the JWICS program manager.

m. **Joint Deployable Intelligence Support System.** JDISS is a standard UNIX multifunctional workstation. JDISS uses commercial off-the-shelf hardware and software to provide a consistent user interface and interoperable applications across commands. JDISS is the joint standard workstation for DOD intelligence. All unified commands and subordinate commands use JDISS.

n. **Frequency Resource Record System (FRRS).** FRRS is a virtual address extension and/or video management system application to support national and combatant commander frequency managers. It includes a frequency assignment data base, a proposal preparation and validation capability, Defense Secure Network connectivity, and proposal coordination and approval notification.

o. **Global Positioning System (GPS).** GPS provides users with their latitude, longitude, altitude, and velocity. Secondly, GPS detects nuclear detonations and transmits the detonation locations and characteristics to proper authorities. Finally, GPS provides precise global time.

p. **Defense Satellite Program (DSP).** DSP is a space-based satellite system designed to detect and report missile launches. Launch data is down-linked to processing stations, evaluated, then

forwarded to strategic and theater users. Primary means of disseminating launch information to the geographic combatant commanders is from US Space Command's (USSPACECOM's) Theater Event System over two separate UHF broadcast systems.

q. **Defense Meteorological Satellite Program (DMSP).** The only DOD weather satellite system, DMSP provides a 1400 nautical mile swath coverage twice daily. Weather images (infrared and visual) are transmitted real time to tactical receivers during each satellite pass. Information provided includes atmospheric moisture altitude profile, cloud cover and environmental information.

r. **Fleet Satellite Communications System** is comprised of the FLTSATs, LEASATs, GAPFILLERs, and UFO satellites. These satellites are positioned to provide UHF satellite communications from 70 degrees north to 70 degrees south latitudes over four areas of service: CONUS, Atlantic Ocean, Indian Ocean, and the Pacific Ocean. The system provides a variety of long haul, point-to-point broadcast and netted single-channel communication links among mobile and shore units. The US Navy and other DOD users interface through the Fleet Satellite Communications system into the DISN and the Naval Telecommunication System.

- The LEASATs are leased commercial satellites designed as a supplemental system augmenting the FLTSATs to ensure fulfillment of non-strategic MILSATCOM requirements. Each LEASAT provides users 13 discrete channels with frequencies ranging from 240 to 320 Mhz.

- The GAPFILLERs are leased UHF payloads on maritime satellites as a temporary service designed to fill the "gap" in UHF MILSATCOM between the previous TACSATs and the FLTSATs.

s. **Public Switched Telephone Network (PSTN).** PSTN is routinely used by the military for a myriad of purposes. The PSTN is a highly competitive but smoothly integrated mix of long-distance carriers, regional operating companies, and local service providers. Alongside familiar technologies such as secure and nonsecure voice and FAX, military users increasingly depend on new categories of service, including pagers, cellular telephones, high capacity data links such as fractional T-1, T-3, Integrated Services Digital Network, Asynchronous Transfer Mode, and video teleconferencing.

t. **Submarine Cable.** Submarine cable is one of the oldest, most reliable long-haul communications systems available. Submarine cable systems are used as part of the DISN system and provide links from CONUS to Europe, the Caribbean, and the Pacific.

u. **Improved Emergency Message Auto Transmission System (IEMATS).** IEMATS provides the Joint Staff and single integrated operations plan combatant commanders with automated emergency action message processing capability. IEMATS allows rapid composition, review, release, receipt, and acknowledgment of emerging actions messages and automatic injection into supporting C4 transmissions means.

4. Service C4 Systems

C4 service systems support strategic-through tactical-level requirements including satellite earth terminals and telecommunications facilities.

a. **Army Systems**

- Army operational- through tactical-level C4 systems are designed to support units from an Army Forces (ARFOR) headquarters down to the rifle squad. To

meet these divergent organizational needs for voice, message, video and data, the Army relies upon three primary tactical communications systems: Tri-Service tactical communications (TRI-TAC) for echelon above corps, mobile subscriber equipment (MSE) for corps and division-size units (with network access extending down to brigade and battalion level), and Single-Channel Ground and Airborne Radio System (SINCGARS) for combat, combat support, and combat service support units at brigade, battalion, and lower levels.

- To meet the Army Service component command or numbered Army crisis C2, the Army deploys a uniquely designed signal company, the Power-Pac Company. This company includes long-haul military and commercial satellite communications that interface with commercial and JTF networks. This includes single-channel (UHF and INMARSAT) radio and tri-band commercial satellite terminals. The commercial satellites operate in the C- and Ku-bands while the military SHF satellites (DSCS) operates in the X-band. TRI-TAC and commercial switching equipment will interface with joint communications. In addition, modern computers that switch data from within the theater to CONUS is part of the equipment suite.

- The TRI-TAC trunking and switching networks at Army Service component command or numbered Army, echelon above corps, and the MSE radio telephone and/or packet switching system at corps, division, and/or brigade echelons provide the existing backbone network for Army C4I. These systems perform circuit or packet switching and handle user-operated radios or wire line voice, record, data, and facsimile traffic. TRI-TAC can also perform message switching using the AN/TYC-39.

- In a joint environment, the Army's voice, message, and data traffic is routed from subordinate echelons through the Army force headquarters to the JTF switches, and into the DISN over commercial or military satellite systems. The ARFOR can also route trunks directly from an operations area into the DISN using its own GMF satellite communications or commercial satellite equipment. Usually, some trunks on Army systems are designated as joint circuits and are used by the JTF, other Services, and special operations forces (SOF).

- With the appropriate crypto keys, Army MSE operates up to the top secret level. TRI-TAC can operate at the top secret and compartmented levels.

b. **Navy Systems**

- **Command Information System.** Command information system is the command, control, and intelligence implementation of the Navy's COPERNICUS strategy for a common C4I architecture to provide the common tactical picture. Command Information system uses a COE, common application programming interfaces, common integration standards for developers and a common human and/or computer interface to ensure modularity and functional interoperability between various applications at all levels of command.

- **Navy Tactical Command System-Afloat (NTCS-A).** NTCS-A is the afloat segment of the command information system architecture and is GCCS COE-compliant. It provides the tactical commander with timely, accurate, and complete all-source information management, display, and dissemination capabilities. These include multi-source data fusion and distribution of

command, surveillance, and intelligence data and imagery to support warfare mission assessment, planning, and execution.

- **Joint Tactical Information Distribution System (JTIDS).** JTIDS/Link-16 is a high capacity digital information distribution system that provides rapid, secure, jam-resistant (frequency hopping) communications, navigation, and identification capabilities to tactical users.

- **Joint Maritime Communications System (JMCOMS).** JMCOMS provides an integrated network manager and associated interfaces to dynamically manage afloat radio frequency (RF) bandwidth requirements over the entire RF spectrum in use by forces afloat. By standardizing the way in which all computer data (tactical, messaging, administrative) is packetized, the shipboard integrated network manager may then determine, using various criteria (priority, amount, address), over what RF media the data will be routed automatically. This will provide a tactical Internet Protocol network to forces afloat. In addition, the integrated network manager will also implement an automated tactical voice and video network.

- **Digital Wideband Transmission System (DWTS).** DWTS provides secure, bulk-encrypted voice and data, ship-to-ship and ship-to-shore communication at data rates up to 2.048 Mbps, operating over UHF line-of-sight (LOS). This system is also capable of supporting conditioned diphase, full duplex, TRI-TAC communications. DWTS provides the necessary communications path to support joint task force, amphibious task force, and landing force staffs in the planning and execution of expeditionary warfare operations.

- **Challenge Athena** provides full duplex, commercial satellite T-1 throughput to afloat warfighters. It allows shipboard communicators to allocate bandwidth and channel assignments to fit mission priorities.

c. **Air Force Systems**

- Air Force C4 systems provide support from strategic to tactical levels, including the support of the DISN and a major role supporting the orbital management and control of space-based C4 resources.

- The Air Combat Command's Wing Initial Communications Packages and the Air Mobility Command's Mobility Initial Communications Kits will deploy to support the air wings. The Wing Initial Communications Package includes a small group of communicators and lightweight communications equipment for initial installation at a deployed air base. The equipment comprises both single- and multi-channel satellite systems for the transmission of voice, message, and data. The equipment also includes secure and nonsecure telephone and facsimile equipment. Once the initial deployment is completed, elements of the Combat Communications Groups, the 3rd at Tinker AFB, OK, and the 5th at Warner Robins AFB, GA, (augmented by eight Air National Guard combat Communications Groups), will deploy more capable communications equipment to support the mission.

- The Air Force, like the Army, is replacing older TRI-TAC AN/TTC-39 voice and AN/TYC-39 message switches and the AN/TSC-94/-100 GMF satellite communications terminals with state-of-the-art digital equipment. It is procuring commercial telephone switches and lightweight, multi-band satellite terminals. The switches are capable of

entering the DISN or PSTN. The multi-band satellite equipment is capable of operating in the C-, Ku-, or X-bands. The satellite equipment provides integral voice and data switching capability.

- The Theater Air Control System (TACS) provides the Air Force component commander and the joint force air component commander with the capability to plan and conduct theater air operations. Ground elements of the TACS include the Air Operations Center, Air Support Operations Center, Tactical Air Control Party, and Control and Reporting Center and/or Element. Airborne elements include the Joint Surveillance and Target Attack Radar System, Airborne Warning and Control System, Airborne Battlefield Command and Control Center, Forward Air Controller Airborne, and Tactical Air Controller Airborne. The Air Operations Center is the senior element of the TACS.

d. **The Air Operations Center**

- The Air Operations Center replaces the Tactical Air Control Center.

- When providing service to the JTF Air Force component commander, the Air Operations Center may require satellite links back to the unified command Air Force component commander. Currently, these "Reachback" links are provided through the DSCS satellite system or commercial satellite equipment.

- Multiband Satellite Terminals and Theater-Deployable Communications packages provide connectivity to commercial and DISN networks and deployed wing locations. TRI-TAC equipment will provide connectivity to the JTF and other Service component headquarters.

- Communications with and from the Air Force Combat Control Teams to the Army and Marine Corps units include HF radio and UHF single channel satellite for long-haul communications. UHF and VHF LOS communications equipment provide for air-to-ground operations.

- The Theater Battle Management Core System supports the Air Operations Center by providing force level planning and execution through the Contingency Theater Automated Planning System, Wing Command and Control System, global mobility command and control through the Command and Control Information Processing System, and theater-wide intelligence analysis and dissemination through the Combat Intelligence System capabilities.

e. **Marine Corps Communications**

- The Marine Corps' combat-ready Fleet Marine Forces are organized into Marine air-ground task forces (MAGTFs). All MAGTFs consist of a command element, ground combat element, aviation combat element, and a combat service support element. MAGTFs can be task-organized as required.

- At the MAGTF headquarters level, and in some cases at subordinate element levels, Marine Corps tactical communications can interface with the DISN, the Naval Telecommunications System, and with other US military tactical communications systems.

- GMF satellite equipment is organic to a Marine expeditionary force. During contingency operations, the MAGTF headquarters can connect to DISN common-user services through a GMF satellite gateway or HF radio link. The limited information throughput of HF

radio usually precludes HF radio as the primary DISN entry for large MAGTFs. GMF satellite equipment is also used to interconnect widely dispersed subordinate elements with headquarters. A JTF's subordinate MAGTF, which is located beyond the terrestrial wide band multi-channel range, will also be interconnected by a satellite link. The GMF equipment used to establish the JTF-MAGTF communications link is normally provided by the JTF from JCSE assets.

- A MAGTF may enter the Naval Telecommunications System by way of a transportable Common-User Digital Information Exchange System or by HF radio to the Naval Computer and Telecommunications Area Master Station. Deployable UHF satellite systems also allow access to the Navy's High Speed Fleet Broadcast and Fleet Secure Voice communications systems.

- A MAGTF and its subordinate elements are equipped with TRI-TAC compatible circuit switches and the Unit Level Circuit Switch. These switches are linked by a digital wide band terrestrial backbone consisting of LOS equipment and troposcatter systems. Using this equipment, a deployed MAGTF possesses a high-capacity digital switching and trunking system capable of providing the MAGTF commander and subordinate elements with secure voice, data, facsimile, and messaging capabilities. This digital network is interoperable with TRI-TAC and, through an appropriate gateway, with DISN.

- MAGTF elements also possess a variety of single-channel combat net radios that include VHF SINCGARS, portable and vehicular-mounted HF sets, portable and shelter-mounted LOS radios, and single-channel satellite UHF radios. Additionally, the Marine Corps will field HAVE QUICK compatible UHF radios.

- The Marine Air Command and Control System has been in existence since the mid-1960s and is still the principal MAGTF Aviation Combat Element command and control system. Compatible with the Navy Tactical Data System, the Marine Air Command and Control System uses standard data links to exchange and process aviation combat information between Marine, Navy, Air Force, Army anti-air combat units, and North Atlantic Treaty Organization combat aviation and aviation command and control facilities.

5. The Joint Staff

Under the direction of the Chairman of the Joint Chiefs of Staff, the Joint Staff develops, recommends, and coordinates policies for C4 systems and assets controlled by the Chairman. The J-6 develops and coordinates policies, maintains surveillance over the readiness of these assets, and develops recommendations for tasking these assets. The Operations Division (J-3) establishes priorities for competing requirements and makes recommendations when requests do not comply with established policy. The J-3 also directs the deployment of JCSE assets after proper approval. CJCS Instruction 6110.01, "CJCS-Controlled Tactical Communications Assets," governs the deployment of C4 assets controlled by the Chairman. CJCSI 6110.01, "CJCS-Controlled Tactical Communications Assets," also provides a detailed description of how to obtain support and the scaleable capabilities of significant C4 assets, specifically the JCSE.

Intentionally Blank

APPENDIX A
C4 PLANNING CONSIDERATIONS

1. Purpose

This appendix provides C4 planners with questions to assist their planning efforts. The list is by no means definitive. It simply serves as a starting point.

2. General

a. C4 planning is inextricably linked with operations planning. The goal of C4 planning is to support mission accomplishment. The mental process C4 planners use is generally the same regardless of the mission or geographical area. Although the checklist has a joint perspective, it can be applied to other C4 staffs — single-Service, subordinate component, and multinational.

b. Numerous sources of information may be used to answer the checklist questions. The following list is representative.

- Existing operation plans and operation orders.
- The JFC's planning guidance, estimate, intent, and concept of operations.
- Area studies.
- Unit files.
- CJCSM 6230.01, "C4 Planners Handbook."
- CJCSM 6231, "Manual for Employing Joint Tactical Communications."
- CJCSM 6230.04, "Manual for Employing Revised Battlefield Electronic CEOI Systems."
- CJCSM 6230.05, "Joint Have Quick Planners Manual."
- DISA Contingency Plan 10-95.
- "Joint Communications Support Element Planning Guide."
- Lessons-learned data bases from previous operations and exercises, especially the Joint Universal Lessons Learned System.
- Systems Description Document Volume I & II.
- Time-phased force and deployment data and time-phased force and deployment list.
- Joint Pub 5-00.2 "Joint Task Force Planning Guidance and Procedures."

3. Common Questions

These questions apply to any mission. They elicit background information, and each serves as a data point to answer other questions.

a. **Parameters**

- What is the JTF mission?
- What is the signal and/or communications unit mission?
- What is the geographic operational area?
- What is the JFC's estimate of the mission and vision (intent and concept of operations) to accomplish it?
- What are the JFC's C4 requirements?
- Who are the subordinate component and supporting forces? What are the command relationships?

- How will the forces deploy (means of transport), and what is the deployment time line?
- Are there any transport and/or lift restrictions (availability of assets, departure and arrival locations)?
- Are there any satellite landing rights?
- When are the operations planning meetings scheduled? How will C4 planning meetings fit into this schedule? Has DISA been involved regarding coordination of technical requirements?
- Are there any planning constraints?
- Are there any special C4 requirements? Who has them?
- What national space-based assets are required and/or available to support the operation? Has a USSPACECOM Joint Space Support Team been contacted?
- What C4 capabilities are available to the joint force: SHF and/or UHF commercial satellite, DSCS, fleet satellite communications, MILSTAR satellite terminals, JWICS, MILSTAR, HF and VHF radio, tropospheric and LOS microwave systems, LANs and WANs, AUTODIN, DISN, land mobile radio, personal communications systems?
- What frequencies are available for the joint operations area?
- What are the general communications security (COMSEC) requirements? Will the Intertheater Communications Security Package (ICP) be used? Who will draft the callout message?
- Who is the potential adversary? What are their capabilities to conduct offensive information warfare? Does a joint force plan exist to counter the threat?
- What are the releasability requirements for multinational operations?

b. **Subordinate Component Forces**

- Where will their C4 nodes be located?
- What are their C4 requirements?
- What are their C4 capabilities?
- What type of C4 systems do they have (power, frequency bands, interoperable and compatible with other subordinate components' equipment, mobility)?
- Who is the component C4 staff point of contact for planning and technical management and direction?
- Are there any special C4 requirements resulting from the mission and the JFC's estimate, intent, and concept of operations?
- Are subordinate and supporting C4 plans consistent with the supported JFC's C4 plan?

c. **Supporting Forces and Activities**

- What is the mission of the supporting forces and/or activities (this includes allies and coalitions)?
- What are their C4 capabilities?
- What information does the supported JFC need from the supporting forces and/or activities (intelligence, weather, imagery, mapping, deployment) and how will it be accessed?
- What C4 support will the supporting forces or activities require from the supported JFC?

d. **Non-organic C4**

- **DISA**

  •• Does the operational area have a DISA Regional Control Center or field office?

  •• Who is the DISA point of contact?

  •• What is the DISN infrastructure in the operational area?

  •• Are sufficient gateways available? What are the interface requirements to access the gateways? Is the equipment available?

  •• Is Telecommunications Service Provisioning and/or National Security Emergency Preparedness involving authority provided and current?

  •• What are the anticipated DSCS and commercial satellite requirements?

  •• Has modeling of space networks been initiated by DISA?

- **Commercial Networks**

  •• Are commercial networks available for use? Who can approve access to them? Are funds available? Has DISA been contacted to ensure required lead times for normal allocations? (1) Satellite (2) Data (3) Voice?

  •• What special interfaces are required to access the commercial network and where are the access points?

  •• What are the locations and types of switches in the commercial network? What are their technical parameters?

  •• Where are the locations and types of systems providing the backbone transmission network?

  •• What type of power is used — voltage, current, commercial grid, or generator?

  •• Does the operational area have a cellular network? What are the transmission media, frequency band, and interface requirements? What are the system standards? Is the system available for use?

- **CJCS Controlled C4 Assets**

  •• What CJCS controlled assets are available?

  •• What capabilities are available?

  •• Will JCSE support be required in the operational area, or will other defense and commercial assets be sufficient?

  •• Will JCSE support be needed for en route communications?

  •• Has a CJCSI 6110.01, "CJCS-Controlled Tactical Communications Assets," support request for CJCS controlled C4 assets been submitted?

  •• What are the JCSE's logistic support and electrical power requirements?

  •• What are the JCSE airlift considerations, allocations, and/or priority?

- **Other C4 Support**

  •• Is C4 support needed from specialized communications units?

•• Who are the points of contact (POCs), and what are the request procedures?

•• What are the units' C4 capabilities and limitations?

4. Planning Activities

This paragraph assumes that the basic questions have been answered and covers high-level and detailed C4 planning. Although these functions are listed separately, they are concurrent rather than sequential actions. The planners interact to refine the planning products, C4 estimates, Annex K, and JCEOI.

a. **High Level Planning**

- What nodes will be necessary to provide a global C4 network and where will they be located?
- Which nodes will have to be connected?
- What transmission media will be used to interconnect the nodes?
- What types of C4 equipment will be located at each node (equipment strings, interoperability of the equipment)?
- What are the frequency requirements for each node? How will the frequencies be allotted (joint, multinational, and subordinate components)? Are there potential frequency conflicts?
- What are the call signs and/or words for each node?
- What units will provide, install, operate, and maintain the equipment for each node? What is their operational readiness status?
- What lift assets are available to deploy these units? When will the units deploy and activate the nodes or network?
- Is the deployment schedule of C4 assets consistent with the phases of the plan? Will it permit the provision of C4 support when and where needed?
- What is the phased buildup of C4I in the operational area?
- Has C4 scheduling information been added to the time-phased force and deployment data and/or time-phased force and deployment list?
- Have the JFC and J-3 been informed of potential C4 shortfalls and recommended solutions?
- How will keying material be managed (ordering, generation, storing, distribution, transferal, and destruction)? What are the procedures for handling compromises? Is a COMSEC logistics management activity needed in the joint operations area? What access will allies have to US COMSEC?
- Are network and node diagrams available?
- Have special C4 requirements been addressed (search and rescue, SOF, en route C4, embarkation and debarkation connectivity)?
- How will the joint, JSOTF, subordinate component, and supporting forces networks interface with non-organic networks (DISN, commercial, JCSE)?
- When and where will the Joint Communications Control Center be established?
- Are the subordinate component, JSOTF, and supporting C4 plans consistent with the joint C4 plan?

b. **Detailed Planning**

- **Circuit Switches**

  •• Does a circuit switch network diagram exist that shows information about the switch and circuit switch network connectivity (switch type, area code, trunk groups, capacity)?

  •• How does the switch route calls: flood, deterministic, or circuit switch routing task execution plan?

  •• Where do circuit switches need to be located? How will they be connected?

  •• What special features or restrictions will be imposed on subscribers? Who will authorize and enforce these restrictions?

  •• Where are the Defense Switched Network (DSN) interfaces? Are precedences authorized? By whom?

  •• How will subscriber assistance be handled?

  •• Where is the greatest anticipated traffic load? Does sufficient capacity exist to handle it?

  •• What types of status reports are required, and when will they be submitted?

  •• How will traffic metering and network loading be measured, modeled, and managed?

  •• Who will publish telephone directories and how will they be distributed?

- **Data Networking**

  •• What is the anticipated JTF component data requirements?

  •• Has automation been planned and/or engineered into the network (x.25, IEEE 802.3, TCP/IP)?

  •• What and/or where are the network identifications and gateways?

  •• Will data of various classifications "ride" a secure tactical backbone? How will traffic of various classifications be controlled and managed? Are multi-level information systems security initiative devices needed and are resources available?

  •• What is the joint architecture topology?

  •• Who is the joint data networks manager?

  •• What are the NIPRNET, SIPRNET, and JWICS connectivity requirements?

  •• What Integrated Tactical Strategic Data Networking points of presence will be used? Has a gateway access request been submitted in accordance with DISA contingency and/or exercise plans?

  •• What is the addressing scheme?

- **Message Switches**

  •• Where are the message switches required?

  •• What is the trunking plan?

  •• What is the network connectivity of all message switches?

  •• Have routing indicators been developed and routing tables established?

  •• Is this an R and/or Y network?

  •• Has a plain language address directory been created?

•• How will special category traffic be handled? Who will be authorized to have access?

•• What are the intranodal and internodal terminals?

•• What types of status reports are required and when will they be submitted?

•• What AUTODIN Switching Centers are connected to the message switch?

•• Who is the Automated Message Process System Security Officer?

•• Who will act as the AUTODIN controller?

- **Transmission Systems**

•• Are the circuit requirements, routing, channelization, and other parameters identified in high-level planning valid? Have satellite access requests been submitted? Have frequency requests been approved and published?

•• What are the characteristics and connectivity of multiplexers in the network? Are they compatible?

•• What are the timing requirements for the network components? How will timing be accomplished?

•• What types of status reports are required and when will they be submitted?

5. Technical Management and Direction

a. **Joint Communications Control Center**

- What are the operational procedures for the JCCC?
- How will the JCCC be manned?
- What reports will be required, how often will they be required, and when will they be submitted?
- How will network reconfiguration be accomplished?
- Who are the POCs at the subordinate control centers?
- Who will submit the Telecommunications Service Request and Telecommunications Service Order?
- Who will coordinate changes to connectivity with the DISN? With the commercial networks?
- What kind of statistics will be kept? Who will analyze them? What will be done with them?
- How will changes caused by the evolving tactical situation be handled?
- Can the JCCC direct changes within subordinate component networks to optimize C4 within the joint operations area?
- Where is the boundary between technical direction and operational direction?
- How will frequency deconfliction be managed? How can potential conflicts be anticipated?
- Who will control frequency spares and authorize their use?
- Who manages the allocated satellite bandwidth used by the geographic joint forces?

b. **JCSE**

- Who is the JCSE POC?
- How will JCSE participate in the technical management process?
- Are there any special reporting requirements for systems provided by the JCSE?

6. Other Planning Functions

a. **Spectrum Management**

- What are the provisions and procedures for frequency planning and use for opposed and/or unopposed entry operations into a operational area?
- What frequency allotments and assignments are available for the operational area?
- Can the allotted and assigned frequencies support the equipment deployed to the operational area (communications, computer LANs and/or WANs, sensors, surveillance radars, GPS, airspace control radars)?
- Will the frequencies work (propagation and topographic analyses)?
- Does the allocation and assignment of frequencies to subordinate component commands contribute to mission accomplishment?
- What are the enemy capabilities to interfere with allotted and assigned frequencies? Does a joint plan exist to counter the threat?
- How will Meaconing, Interference, Jamming, and Intrusion (MIJI) be reported?
- Who will submit MIJI reports to the Joint Spectrum Center (JSC)?
- Will the JCCC resolve electromagnetic interference issues? Will JSC support be required to resolve interference issues?
- Are sufficient spare frequencies available?
- What emission control measures will be applied?
- Will the JFC implement an electronic deception plan? Are sufficient frequencies available to support this plan?

b. **Security**

- Will the cryptographic equipment interoperate?
- What are the keying material requirements?
- Does a key management plan exist?
- How will cryptographic compromises be detected and corrected?
- What computer security measures will be employed on the LANs and WANs in the operational area?
- How will access to the various networks be controlled (electronic and physical)?
- Have COMSEC emergency destruction procedures been established?
- What is the logistics plan for the cryptographic equipment?
- Are equipment and keymat sufficient to support planned and unplanned operations?
- Have key change times been established and promulgated?

- Have provisions been made for over-the-air-rekeying where applicable?
- Is an ICP available? Is it needed?
- What will we transition to and when?
- What is the foreign information warfare threat facing the C4I system?
- Are virus detection software applications installed and operational? Are passwords issued and in use? Has a contingency plan been developed to guide recovery actions should data be modified or destroyed by unauthorized intrusions?
- Do remotely accessed computer systems possess features to identify users and substantiate their identification before allowing information to be processed?

7. Summary

This list of questions is not all-inclusive. These questions should be asked repeatedly throughout the planning process as C4 planners adapt to an evolving operational and tactical situation. They provide a framework for supporting C4 planning for each phase of an operation, focusing C4 planners on the mission and how the JFC intends to accomplish it.

APPENDIX B
REFERENCES

The development of Joint Pub 6-02 is based upon the following primary references.

1. DOD Directive 3222.4, 31 July 1992, "Electronic Warfare (EW) and Command, Control and Communications Countermeasures (C3CM)."

2. DOD Directive TS-3600.1, 21 December 1992, "Information Warfare (U)."

3. DOD Directive 5000.1, 23 February 1991, "Defense Acquisition."

4. DOD Directive 5105.19, 25 June 1991, "Defense Information Systems Agency (DISA)."

5. DOD Directive 5137.1, 12 February 1992, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I])."

6. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations."

7. CJCSI 3210.01, "Joint Information Warfare Policy."

8. CJCSI 3213.01, 28 May 1993, "Joint Operations Security."

9. CJCSI 5112.01, 19 September 1994, "Charter for Theater Air Defense Battle Management Command, Control, Communication, Computers, and Intelligence Joint Oversight Committee."

10. CJCSI 6110.01, 25 January 1996, "CJCS-Controlled Tactical Communications Assets."

11. CJCSI 6211.02, 23 June 1993, "Defense Information Systems Network and Connected Systems."

12. CJCSI 6212.01A, 30 June 1995, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers and Intelligence Systems."

13. CJCSI 6510.01, 1 September 1993, "Defensive Information Warfare Implementation."

14. CJCSM 6230.01, "C4 Planners Handbook."

15. CJCSM 6230.04, "Manual for Employing Revised Battlefield Electronic CEOI Systems."

16. CJCSM 6230.05, "Joint Have Quick Planners Manual."

17. CJCSM 6231, "Manual for Employing Joint Tactical Communications."

18. CJCSM 6231.01, 17 March 1995, "Manual for Employing Joint Tactical Communications Systems/Joint Communications Systems Architecture and Management."

19. CJCSM 6231.07, 1 May 1995, "TRI-TAC Equipment, Volume VII, Network Management."

20. CJCS MOP 6, 3 March 1993, "Electronic Warfare (U)."

21. CJCS MOP 30, 8 March 1993, "Command, Control, and Communications Countermeasures."

22. CJCS MOP 31, 8 May 1992, "Submitting and Assigning Priorities to Requirements for Mapping, Charting, and Geodesy Support."

23. CJCS MOP 37, 14 May 1992, "Military Satellite Communications Systems."

24. DISA Contingency Plan 10-95.

25. Joint Pub 1, "Joint Warfare of the Armed Forces of the United States."

26. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

27. Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms."

28. Joint Pub 3-0, "Doctrine for Joint Operations."

29. Joint Pub 3-05, "Doctrine for Joint Special Operations."

30. Joint Pub 3-13.1, "Joint Doctrine for Command and Control Warfare Operations (C2W)."

31. Joint Pub 3-51, "Electronic Warfare in Joint Operations."

32. Joint Pub 3-54, "Joint Doctrine for Operations Security."

33. Joint Pub 3-56, "Command and Control Doctrine for Joint Operations."

34. Joint Pub 4-0, "Doctrine for Logistic Support of Joint Operations."

35. Joint Pub 5-0, "Doctrine for Planning Joint Operations."

36. Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures."

37. Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations."

APPENDIX C
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Command, Control, Communications, and Computer Systems (J-6).

3. Supersession

This publication supersedes Joint Pub 6-02, 1 April 1968, "Joint Doctrine for Operational/ Tactical Command, Control, and Communications Systems" and MCM-008-91, 16 January 1991, "Contingency Communications Between the Commander of a Joint Task Force and a US Diplomatic Post."

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J6/J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington, D.C. 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center 2800 Eastern Boulevard Baltimore, MD 21220-2898
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, D.C. 20593-0001

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY
PART I—ABBREVIATIONS AND ACRONYMS

AMPE	automated message processing exchange
ARFOR	Army forces
AUTODIN	automatic digital network
C2	command and control
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CJCS	Chairman of the Joint Chiefs of Staff
COE	common operating environment
COMSAT	communications satellite
COMSEC	communications security
CONUS	continental United States
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMS	Defense Message System
DMSP	Defense Meteorological Satellite Program
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DSCS	Defense Satellite Communications System
DSP	Defense Satellite Program
DSSCS	Defense Special Security Communications System
DWTS	Digital Wideband Transmission System
EHF	extremely high frequency
EM	executive manager
EMI	electromagnetic interference
FLTSAT	fleet satellite
FRRS	frequency resource record system
FTS	Federal Telecommunications System
GBS	Global Broadcast System
GCCS	global command and control system
GMF	ground mobile forces
GPS	global positioning system
HF	high frequency
ICP	Intertheater COMSEC Package
IEMATS	Improved Emergency Message Auto Transmission System
INMARSAT	International Maritime Satellite

INTELSAT	International Telecommunications Satellite Organization
IW	information warfare
IW-D	defensive information warfare
J-3	Operations Division
J-6	C4 Systems Division
JCCC	joint communications control center
JCEOI	joint communications-electronics operating instructions
JCSE	Joint Communications Support Element
JDISS	Joint Deployable Intelligence Support System
JFC	joint force commander
JMCOMS	Joint Maritime Communications System
JSC	joint spectrum center
JSMS	Joint Spectrum Management System
JSOTF	joint special operations task force
JTF	joint task force
JTIDS	Joint Tactical Information Distribution System / Link 16
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LEASAT	leased satellite
LOS	line-of-sight
MAGTF	Marine air-ground task force
Mbps	megabytes per second
Mhz	megahertz
MIJI	meaconing, interference, jamming, and intrusion
MILSATCOM	military satellite communications
MILSTAR	military strategic and tactical relay system
MSE	mobile subscriber equipment
NCA	National Command Authorities
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NTCS-A	Navy Tactical Command System Afloat
POC	point of contact
PSTN	Public Switched Telephone Network
RF	radio frequency
SCI	sensitive compartmented information
SHF	super high frequency
SINCGARS	Single-channel Ground Airborne Radio System
SIPRNET	Internet Protocol Router Network - Secret Level
SOF	special operations forces
STU-III	secure telephone unit-III
SVS	secure voice system
SYSCON	system control

TACS	Theater Air Control System
TACSAT	tactical satellite
TRI-TAC	Tri-Service Tactical Communications
UFO	UHF Follow On
UHF	ultra high frequency
USSPACECOM	US Space Command
VHF	very high frequency
WAN	wide area network

PART II—TERMS AND DEFINITIONS

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is a warfighting application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C2 system. (Joint Pub 1-02)

common operating environment. The common operating environment provides a familiar look, touch, sound, and feel to the commander, no matter where the commander is deployed. Information presentation and command, control, communication, computers, and intelligence system interfaces are maintained consistently from platform to platform, enabling the commander to focus attention on the crisis at hand. Also called COE. (Approved for inclusion in the next edition of Joint Pub 1-02.)

communicate. To use any means or method to convey information of any kind from one person or place to another. (Approved for inclusion in the next edition of Joint Pub 1-02.)

computer security. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. (Approved for inclusion in the next edition of Joint Pub 1-02.)

deployment planning. Operational planning directed toward the movement of forces and sustainment resources from their original locations to a specific operational area for conducting the joint operations contemplated in a given plan. Encompasses all activities from origin or home station through destination, specifically including intra-continental United States, intertheater, and intratheater movement legs, staging areas, and holding areas. (Joint Pub 1-02)

information warfare. Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems. Also called IW. (Joint Pub 1-02)

global grid. An open systems architecture that provides global connectivity instantaneously on warrior demand. The global grid can support both vertical and horizontal information flow to joint and multinational forces. (Approved for inclusion in the next edition of Joint Pub 1-02.)

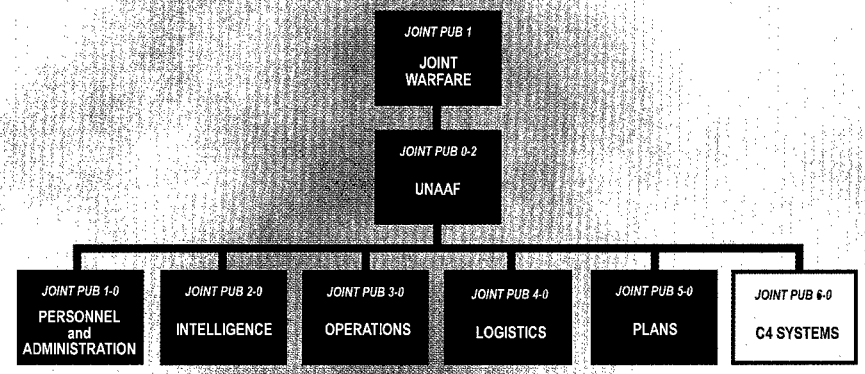
joint communications control center. An element of the J-6 established to support a joint force commander. The Joint Communications Control Center (JCCC) serves as the single control agency for the management and direction of the joint force command, control, communications, and computers systems. The JCCC may include plans and operations

administration, system control, and frequency management sections. Also called JCCC. (Approved for inclusion in the next edition of Joint Pub 1-02.)

node/command, control, communications, and computers node. The physical and functional grouping of communications and computer systems that provide terminating, switching, and gateway access services to support information exchange. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 6-02** is in the **C4 Systems** series of joint doctrine publications. The diagram below illustrates an overview of the development process: